UNIVERSIDAD CARLOS III DE MADRID

TESIS DOCTORAL

Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red. Aplicación al Pago Electrónico en entornos Inalámbricos

Autor:

D. Joaquín Torres Márquez

Director:

D. José María Sierra Cámara

DEPARTAMENTO DE INFORMÁTICA

Leganés, Octubre 2006

TESIS DOCTORAL

Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red. Aplicación al Pago Electrónico en entornos Inalámbricos

Autor: D. Joaquín Torres Márquez

Director: D. José María Sierra Cámara

Firma del Tribunal Calificador:

Firma

Presidente:

Vocal:

Vocal:

Vocal:

Secretario:

Calificación:

Leganés, de de

Dedicatoria

Agradecimientos

Índice General

Índice de Figuras

Índice de Tablas

Resumen

En la actualidad, la importancia de la seguridad de la Información y de las Comunicaciones resulta incuestionable. En este contexto, la relevancia de la autenticación fiable entre entidades queda también patente en una diversidad de aspectos cotidianos. Por sus cualidades y ventajas como módulo criptográfico, la tarjeta inteligente ha desarrollado un papel fundamental en la autenticación de usuarios. Esta tesis doctoral estudia el proceso de transformación que está atravesando actualmente y que la convierte en un equipo con conectividad a la red, dentro de la *Nueva Generación de Tarjetas Inteligentes*. De esta evolución, resultan una variedad de implicaciones, que se expanden transversalmente desde el momento que dicha tarjeta se integra en la red. En el presente trabajo se trata dicha integración exclusivamente desde la perspectiva de los mecanismos de autenticación involucrados. Pero, ¿hacia dónde evoluciona esa red?. Una diversidad de redes de acceso, entre las que destacan las tecnologías inalámbricas y los dispositivos multimodo, van a conformar un panorama global del que las tarjetas inteligentes, actuales y futuras, deberán participar. ¿Se pueden hacer más robustos y seguros los esquemas actuales de autenticación remota para éstas?. ¿En qué medida han sido diseñados para ser adaptados a estas nuevas circunstancias?. Esta tesis aborda la problemática de una forma conjunta, atendiendo al esquema de autenticación extremo-a-extremo y plantea un nuevo *Marco de Autenticación para Tarjetas Inteligentes en Red* bajo cuyo paraguas podemos modelar, analizar e incluso proponer una arquitectura de protocolos de autenticación remota para las tarjetas inteligentes actuales y venideras. Tras el diseño y la implementación acorde con dicha arquitectura y una evaluación de las funcionalidades previstas, se realiza una aplicación sobre un escenario realista de pago electrónico en entornos inalámbricos; por un lado demostrando la viabilidad de la propuesta y, por otro, incidiendo en su versatilidad, que le permite ser robusta ante la transformación que les conduce hacia esa nueva generación.

Capítulo 1.

Introducción

1. Introducción

1.1. Seguridad de la Información y aspectos de uso de las Tarjetas Inteligentes.

En los albores del siglo XXI, ha quedado ampliamente consolidada la inmersión universal en las Tecnologías de la Sociedad de la Información y Comunicaciones. Si bien es cierto, que ha sido, y sigue siendo, una tendencia que queda ratificada por el creciente número de conexiones multimodo a Internet, el importante despliegue en el uso de dispositivos de telefonía móvil o el volumen de información digital gestionada globalmente, también podrían ser factores indicativos de este fenómeno la magnitud de inversiones en este área que las instituciones, públicas y privadas, realizan con el objeto de la mejora de los servicios, en el primer caso, o con el de obtener pingües beneficios, en el segundo.

Sin embargo, este nuevo modo de vida *enredado* en el que *todo* está disponible en *todo momento y en todo lugar* se presenta irremisiblemente asociado a las amenazas contra la seguridad que afectan a la Información y a las Comunicaciones. Estas amenazas pueden quebrar la estructura de seguridad de los sistemas en cualquiera de sus planos que, en definitiva, se traducen más allá de su incidencia individual en considerables pérdidas económicas para las organizaciones. De esta manera, se ven forzadas a identificar, atender y gestionar los, cada vez más frecuentes, incidentes de seguridad.

Por todo ello, la necesidad de implantación de medidas de prevención y protección es cada vez más asumida por los equipos directivos y plasmada en sus Sistemas de Gestión de la Seguridad. Así mismo, también es sabido que el establecimiento de medidas de salvaguarda no elimina la posibilidad de que dichos incidentes se produzcan, pero sí permite limitarlos y mantenerlos en un nivel de riesgo que puede ser asumido por la organización.

La Seguridad de la Información, aunque se centra en la protección de todos los activos de los sistemas de información, puede entenderse como la consecución de un conjunto de determinados servicios se seguridad, de los que pueden extraerse como fundamentales: la confidencialidad, la integridad, la disponibilidad y la autenticación. Van a ser los ataques contra ésta última, la autenticación, los que justifican en gran medida el motor inicial, y posteriormente el trabajo realizado, de esta tesis.

Si por autenticación entendemos el proceso de establecer la confidencia de las identidades de una entidad, por protocolo de autenticación debe entenderse como el proceso de intercambio de mensajes bien especificado que verifica la posesión de un elemento identificativo físico o lógico (*tokens*) por parte de una entidad, para remotamente autenticar a la misma. Algunos protocolos de autenticación también generan claves de cifrado para proteger una sesión completa, de forma que los datos transferidos en dicha sesión quedan criptográficamente protegidos.

Aunque esta definición está extraída de [NIST 800-63], hemos sustituidos el término *usuario* por *entidad*, en tanto que en nuestra opinión los dispositivos también están

asociados a una identidad y, más allá, podrían participar en ciertos protocolos de autenticación de forma autónoma e independiente a la existencia de un usuario.

En lo referido a la autenticación de usuarios, las Tarjetas Inteligentes o *Smart Cards* han desempeñado un papel fundamental en nuestra historia reciente Los enormes progresos en microelectrónica realizados a principios de los años setenta, hicieron posible integrar en un tamaño considerablemente reducido el almacenamiento de datos junto con un microcontrolador, en un único chip de silicio. El registro de la primera patente de tarjeta inteligente (año 1974), el descenso en el precio de los circuitos integrados y la aparición de las primeras memorias no volátiles, fueron otros factores que enmarcaron la antesala de la considerada como 1ª generación de estos dispositivos.

Desde el comienzo de su desarrollo, las tarjetas inteligentes proveían un medio ideal para la criptografía. Podían almacenar de forma segura material criptográfico, claves de cifrado y firma, certificados digitales, contraseñas e incluso, con el tiempo, patrones biométricos [Noo00][San03]; al mismo tiempo, estaban capacitadas para ejecutar algoritmos criptográficos, cada vez más potentes. Por otro lado, destacaban por su forma, tamaño y facilidad de manejo, de tal manera que podían ser empleadas en una variedad de contextos por el usuario. Ésta fue la principal motivación que llevó a los bancos a desarrollar soluciones de seguridad para su empleo en transacciones monetarias. Los bancos franceses fueron los primeros en usar esta tecnología en la década de los ochenta, seguidos por los alemanes. Sería a finales de la siguiente década, la de los noventa, cuando aparecerían en el mercado los primeros monederos electrónicos basados en tarjetas inteligentes; para entonces, las tarjetas multiaplicación, máquinas virtuales sobre el hardware de la tarjeta y la programación orientada a objetos con Java Card, formaban parte ya de la realidad de esta tecnología.

Con estos antecedentes, el *pago electrónico* con tarjetas inteligentes, es y seguirá siendo una de las grandes parcelas de interés, y por tanto de negocio, que se prevé para estos dispositivos. El concepto de *pago electrónico*, que se ha de entender en el contexto de esta tesis, se centra en la autorización de la orden de compra, independientemente de la tecnología de acceso y transporte que le dé soporte (redes cableadas, redes locales inalámbricas, Internet, redes de telefonía fija o móvil, etc.) y, aún más importante, exige además de la presencia de una *tarjeta inteligente bancaria presencial* en el momento del pago, de la que se toma ventaja de sus características inherentes de seguridad. Adicionalmente, se hace necesario que el dispositivo desde el que se realiza dicho pago electrónico sea un Terminal Punto de Venta (TPV). Los esfuerzos de las potentes entidades de servicios financieros, como son el caso de Visa, MasterCard y JCB, quedan plasmados, no sólo en unas especificaciones [EMV] que deberán cumplir estas tarjetas (y los terminales TPVs correspondientes) para su uso como soporte del pago electrónico sino que, además, vienen defendiendo una planificación concreta de su implantación. Así por ejemplo, hoy día todas las tarjetas inteligentes de Visa y Visa Electron deben cumplir con estas especificaciones. Al mismo tiempo, desde 1 de Julio de 2006 la clave pública de la Autoridad de Certificación de Visa, de tamaño entre 1408 y 1984 bits, debe ser incorporada en los chips EMV. Si bien es cierto que el número de estas tarjetas continúa creciendo como soporte de pago electrónico a nivel mundial, sigue percibiéndose una resistencia a la migración desde las tarjetas de banda magnética a estas tarjetas con chip. Cuestiones como el hábito de los usuarios o infraestructuras de negocio, plenamente consolidados, son factores determinantes, a pesar de las graves

fallas de seguridad que las primeras aún conservan. En muchos casos se ha adoptado una solución híbrida que incorpora tanto la banda magnética como el chip.

Paralelamente, el *comercio electrónico*[1], por su parte, se ha presentado como un ámbito prometedor para el uso estos dispositivos, encaminados a dotar de seguridad dichas operaciones comerciales, en un entorno en el que el escepticismo y la desconfianza, han sido algunas de las razones que podrían justificar el lento crecimiento de estas compras interactivas *on-line* en algunos países [CMT].

De otro lado, en el marco de las comunicaciones inalámbricas su uso se hace también imprescindible, encontrándose la tarjeta insertada o integrada en el teléfono móvil como Módulo de Identificación del Abonado (SIM en GSM/GPRS o USIM en UMTS). Dicha tarjeta almacena la información personal de éste, credenciales de seguridad, y las preferencias, que pueden ser protegidas por una clave y es posible transportarlas como elemento contractual del abonado con el correspondiente operador de telefonía móvil. En este contexto, las tarjetas inteligentes (U)SIM permiten: el acceso autorizado y autenticado del abonado, políticas particulares de facturación, resolución de políticas de *roaming* entre redes de distintos operadores, así como el acceso seguro a una variedad de servicios móviles emergentes (comercio electrónico móvil, navegación web, servicios de mensajes cortos, etc.).

En los últimos años, el manejo masivo de información sensible, ha permitido el desarrollo y una mejora sustancial en las aplicaciones y protocolos de seguridad de la tarjeta inteligente. En un contexto organizacional éstas permiten: acceso seguro y autenticado de usuarios a sistemas o redes, dependencias corporativas, etc., y en todo caso, almacén y procesado de credenciales y material digital de seguridad. Con la inclusión de las tarjetas inteligentes como un elemento más de la denominada Sociedad de la Información, conviene ahondar en las aplicaciones, protocolos o mecanismos en los que se ponen en juego datos personales y, por tanto, susceptibles de ser protegidos haciendo uso esta tecnología. La importancia de la vinculación entre dicha tarjeta inteligente de forma presencial y la autenticación de usuarios puede verse claramente reflejada en una diversidad de escenarios.

De esta manera, en el plano institucional la tarjeta inteligente como elemento de identificación segura de usuarios está cada vez más presente y, recientemente, la puesta en marcha del DNI electrónico en España o del pasaporte electrónico en otros países del entorno [Rou05][Kle06][Fri06], son buena prueba de ello. Obviamente, el marco legal no ha permanecido ajeno a todos estos procesos tecnológicos que están condicionando el modo de vida de los ciudadanos en casi cualquier parte del mundo. Así, en el caso español la Ley 59/2003, de 19 de diciembre, de firma electrónica contempla, entre otros, dos aspectos directamente relacionados con las tarjetas inteligentes. En el Titulo II de dicha Ley se recogen requisitos y características del Documento Nacional de Identidad Electrónico, que con formato de tarjeta inteligente, deberá acreditar electrónicamente la identidad personal de su titular y permitir la firma electrónica de documentos. A tal efecto, la tarjeta inteligente se convierte en Dispositivo de Firma Electrónica, y en concreto en un Dispositivo de Creación de Firma Electrónica según el Capítulo I, Título

1 Comisión del Mercado de las Telecomunicaciones define el comercio electrónico como *"...toda transacción realizada electrónicamente a través de Internet, excluidas las realizadas en cajeros automáticos, EDI, terminales de telefonía móvil, con independencia del medio de pago utilizado, y del mecanismo de intercambio utilizado (adhesión, subasta, negociación entre las partes, etc.)"*

IV de dicha Ley. Por último, con el Real Decreto 1553/2005, publicado por el BOE el 24 de diciembre de 2005, se regulaba la expedición del Documento Nacional de Identidad (DNI) y sus certificados para la firma electrónica.

Más allá, este proceso de constante evolución de las tarjetas inteligentes tiene dos hitos recientes que lo completan y que en buena medida se constituyen como elementos dinamizadores de su proyección futura. De un lado cabe destacar la trasformación del enlace físico de comunicación entre la tarjeta inteligente y el terminal lector, que culmina con la concepción de una comunicación sin contactos basada en radiofrecuencia; es decir, las *contactless smart cards* en sus distintas versiones (acopladas [ISO/IEC 10536], en proximidad [ISO/IEC 14443] y en vecindad [ISO/IEC 15693]). De otro lado, es necesario permanecer atentos al desarrollo de un nuevo concepto de tarjeta inteligente que desde principios de la presente década está siendo objeto de estudio y de interés por algunos fabricantes: *Network Smart Cards,* es decir, tarjetas inteligentes que incorporan protocolos de capa de red. Estas tarjetas, aunque mantienen un capa física de comunicación basada en [ISO7816] o [USB], aspiran a implementar la pila de protocolos tradicional comúnmente conocida como TCP/IP, lo que la convertiría en un *host* de Internet transportado en nuestra cartera.

Esta revolución en la pila de protocolos de la tarjeta inteligente, sumada a las tendencias que habrán de seguir su interfaz de comunicación, así como una nueva concepción del dispositivo lector han sido enmarcadas en lo que se ha dado en llamar la *Nueva Generación de Tarjetas Inteligentes, NGTI.*

1.2. Nueva Generación de Tarjetas Inteligentes

Aunque hoy por hoy las tarjetas inteligentes son considerados dispositivos avanzados, con interesantes recursos criptográficos y computacionales comparado con su reducido tamaño, el diseño de los protocolos en los que interviene, o incluso las aplicaciones en las que se hace uso, a menudo no han ido más allá de considerarlos como unos elementos de soporte en el esquema global. En este sentido, carecen de la autonomía que se le presupone a cualquier otro nodo de red con capacidad de incorporar protocolos de comunicación acorde con el resto del sistema, cada vez más heterogéneo e interoperable.

Sin embargo, un proceso evolutivo viene detectándose en los últimos años y que, además de los actuales trabajos de investigación y desarrollo alineados y de los intereses de los fabricantes, quedaba ratificado en el informe final del proyecto RESET (Roadmap for European research on Smartcard rElated Technologies) [RES03] de mayo del 2003 y realizado al amparo del V Programa Marco de la Comisión Europea. En este gran proyecto, de un consorcio multidisciplinar y de socios con distinta motivación (academia, fabricantes, operdadores, etc.) se aunaban esfuerzos en pos de intereses comunes. Aunque este informe detalla múltiples aspectos de las directrices que tomará esa nueva generación de tarjetas inteligentes, NGTI, es del interés de nuestro trabajo centrarnos exclusivamente en los aspectos relacionados con la autenticación de los dispositivos que formaran parte de esa generación y que sin duda alguna revolucionarán definitivamente la concepción de esta tecnología

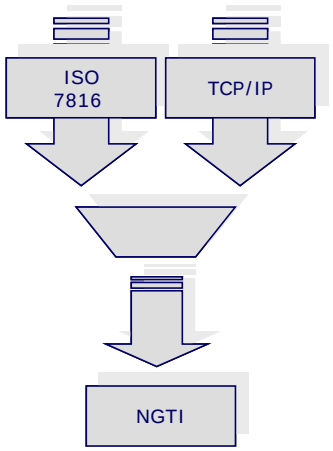

Figura 1.1 Convergencia tecnológica hacia la NGTI con conectividad en red.

Aunque la NGTI abarca un significativo espectro de conceptos y tecnologías, señalamos aquí brevemente las características relevantes para nuestro trabajo, destacando las particularidades que en gran medida lo justifican, con el objeto de identificar las necesidades que de aquí se pudieran derivar. Así, en dicho informe quedaba clara la migración a una tarjeta inteligente con conectividad a la red, que contemple el modelo TCP/IP (Figura 1.1), con la posibilidad de incluir una variedad de protocolos de seguridad en capa de red y superiores (p.e. IPsec, SSL/TLS). Además de interfaces como USB, que hoy por hoy puede considerarse una realidad cercana, el proyecto RESET prevé a largo plazo interfaces de tecnologías como *Bluetooth* o *Wireless* LAN (redes locales inalámbricas). En cuanto a la tecnología de los dispositivos lectores, quedaba contemplada la posibilidad de dotarles de acceso a redes con tecnología UMTS o 4G. De todos estos hechos, el trabajo referido infiere un espectro de oportunidades de negocio que incluye: acceso transparente y ubicuo a e-servicios, interoperabilidad de sistemas, servicios y productos, reducción del tiempo de introducción del mercado a costa de mayor base de desarrollo, etc.

Por último, conviene señalar que aunque esta convergencia de tecnologías acabará siendo una realidad palpable, las estimaciones en su implantación puede ubicarse en el tiempo a medio-largo plazo según las propias estimaciones del grupo de expertos reunidos en torno al proyecto RESET. En la Figura 1.2, se representa la planificación prevista de cada uno de los aspectos que conformarán la NGTI y en donde tal hecho se puede constatar.

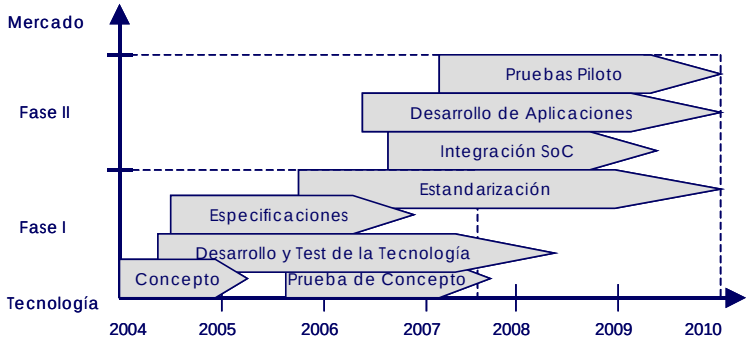

Figura 1.2 Previsión de la planificación e implantación de la NGTI

Atendiendo más específicamente al comportamiento que han de tener los protocolos y mecanismos de autenticación en este proceso de evolución tecnológica, debemos señalar que un dispositivo de la NGTI con las características indicadas, tendrá funcionalidades de seguridad en gran medida parecidas a los actuales dispositivos con conectividad IP, aunque con las limitaciones propias de la capacidad computacional de que disponga.

Nuestro interés, y punto de partida de este trabajo, se centra inicialmente en las soluciones para la integración de forma factible de la *tarjeta inteligente en la red*[2], y más concretamente en los mecanismos de autenticación que ha de soportar la tarjeta para poder acceder a dicha red y a los servicios ofrecidos por ésta. Por integración de la tarjeta inteligente en la red, se habrá de entender en el contexto de esta tesis como la capacidad de ésta de comunicarse en términos de autenticación de forma remota, a través de la infraestructura de red; entendiendo este hecho, como parte de los primeros pasos en esa inercia de las actuales tarjetas inteligentes hacia una nueva generación.

Por tanto, resulta imprescindible tomar en consideración esta proyección tecnológica previsible en las tarjetas inteligentes, para abordar coherentemente nuestro trabajo, asegurándonos que los enfoques y decisiones llevados a cabo en esta tesis son respetuosos con esta evolución y que en modo alguno colisionan con el devenir de esta tecnología, tratando de integrarla de la forma más transparentemente posible.

1.3. Autenticación de Tarjetas Inteligentes a través de la Red en su contexto.

Si bien es cierto que bajo la perspectiva apuntada, la tarjeta inteligente del futuro podrá acceder por ella misma a una red de naturaleza heterogénea como cualquier otro de los dispositivos actuales, todo indica que se tratará de un proceso lento y no exento de dificultades; entre otras, la capacidad computacional y la complejidad que introduce la

[2] Ha de hacerse notar que el concepto de *tarjeta inteligente en red* utilizado en esta tesis no tiene porqué corresponder exclusivamente al término *network smart cards*, sino que es empleado de forma más amplia, al punto de poder considerar la posibilidad de que las actuales tarjetas ISO 7816 puedan acceder a ciertos servicios de seguridad, haciendo uso de la infraestructura de red disponible.

variedad de tecnologías involucradas. Como parece razonable, el resultado final se dará como consecuencia de un conjunto de logros tecnológicos abordables en cada momento y que en definitiva habrá supuesto la suma de diversos procesos de migración. Pero más allá, es necesario considerar que éstos últimos no ocurrirán aisladamente sino que además las tecnologías satélites en torno a la tarjeta inteligente también responderán a sus propios procesos evolutivos con *tempos* particulares. Un breve estudio nos permite identificar factores asociados a estos fenómenos evolutivos:

- Tecnologías heterogéneas: tecnologías de distinta índole se ven involucradas, pudiéndose tratar tanto de las tecnologías relativas a los dispositivos, como de otras propias de redes. Al mismo tiempo, deben contemplarse tecnologías que típicamente soportan servicios que no son del tipo IP y que deberían migrar, dentro de una convergencia común hacia servicios de tipo IP, etc.

- Evolución a distintas velocidades: como cabe esperar, cada una de las tecnologías evolucionan según unos factores y planificación particulares que podrían dificultar una harmonización[3] al unísono. Un rápido vistazo sobre las mismas nos delataría la existencia entre de ellas tanto de tecnologías punteras, y por tanto de reciente trayectoria, como de otras más maduras y de inercias consolidadas. Ha de indicarse también en este punto, que los procesos de implantación de cada tecnología se rigen por sus propias pautas y su materialización en el mercado podría responder a ritmos distintos.

- Asimetría en la aplicación objetivo: para una correcta harmonización entre las tecnologías que convergen en la propia tarjeta, debería ser también necesario el ajuste entre aplicaciones que aspiran a objetivos distintos por su propia naturaleza; así por ejemplo, podemos encontrar aplicaciones de un sector específico frente a otras que pudieran tener un carácter de propósito general.

- Intereses distintos: quizás uno de los factores de más peso para conseguir la armonía de las tecnologías participantes, es el relativo a los distintos intereses que ponen en juego cada uno de los dominios administrativos que podrían verse involucrados. Entiéndase, el desajuste que podrían encontrarse en este sentido entre los intereses relativos al dominio administrativo del terminal lector o al dominio del operador de la red de acceso o el de la red de infraestructura, por ejemplo, que apuntaría hacia potenciales acuerdos tanto en el plano de servicios o negocio, como en el plano legal.

Así, ante el paradigma de la integración de la *tarjeta inteligente en red* cabe preguntarse en primera instancia hacia dónde evoluciona *esa red*. De la certeza y consenso sobre un núcleo de red bajo el paraguas todo-IP caben pocos cuestionamientos. Sin embargo, sobre el de las tecnologías y redes de acceso, en nuestra opinión, conviene detenerse en ellas y entender hacia dónde se dirigen los pasos. Por ser el terminal y red de acceso las

[3] Según la R.A.E: harmonización (o armonización). 1. f. Acción y efecto de harmonizar (o armonizar)

entidades con las que interacciona y comunica directamente la tarjeta inteligente, demandará en nuestro trabajo la atención oportuna.

Al tratarse la tarjeta inteligente de un dispositivo portátil, cabe esperar su utilización en múltiples escenarios de naturaleza variada. Desde el punto de vista de la seguridad, que es donde se centra nuestro trabajo, aquellos en los que se produce la interacción con dispositivos lectores, a priori, **no confiables**, concentrarán nuestros esfuerzos. En una primera aproximación, se pueden considerar los entornos públicos (terminales de acceso/ conexión públicos) como los más representativos de esta circunstancia. Por tanto, resultará de especial interés en nuestro trabajo identificar qué características tendrá el terminal y red de acceso en ambientes públicos que facilitará la comunicación de la tarjeta inteligente con el resto del sistema. Un detallado estudio de los antecedentes y estado de la cuestión en esta materia (capítulo 2), ha sido llevado a cabo para la realización de esta tesis y como se podrá comprobar, las *redes locales*, especialmente las inalámbricas públicas o PWLAN, están marcando un ámbito prometedor para el acceso ubicuo de una variedad de dispositivos, al punto que todo parece indicar que será uno de los escenarios a los que las tarjetas inteligentes deberán enfrentarse.

De otro lado, en el supuesto de que la tarjeta inteligente llegara a integrarse plenamente en la red pública (o incluso privada,) implementado una completa pila estandarizada de protocolos de comunicación y participara como cliente o servidor en un variado conjunto de servicios y aplicaciones, la autenticación remota en el acceso a la red es uno de los retos al que indudablemente habrá de dar respuesta. Al mismo tiempo, de los múltiples servicios que se pudieran proporcionar a través de un tarjeta inteligente en red, el servicio de la autenticación (de usuarios o dispositivos) seguirá siendo, sin duda, del que mejor aprovechamiento pueda hacerse. Por tanto en nuestro trabajo, pretendemos centrarnos en este aspecto como uno de los primeros peldaños en esta evolución de la que estamos dando cuenta, al tiempo que conviene no olvidar en todo este proceso la limitación computacional que se le presupone a una tarjeta inteligente.

Otro de los aspectos que determinan la problemática tiene que ver directamente con el plano de la autenticación en estos dispositivos; en concreto, con el enfoque tradicional de uso de éstos y el diseño tradicional de los protocolos involucrados. Estos hechos son analizados en el siguiente capítulo. La discusión central de ese análisis reside en la alta dependencia existente para con el terminal lector o *host* en los procesos de autenticación y, por tanto, la falta de autonomía, interoperabilidad y flexibilidad que a un dispositivo en red se le exige. Esta dependencia es especialmente no deseable cuando se trata de un terminal en un entorno público cuya confianza puede verse cuestionada en todo momento.

Tras estas consideraciones, en el siguiente epígrafe se detallan los elementos que fundamentan esta tesis y que nos encaminarán hacia el establecimiento de unos objetivos para el desarrollo de la misma.

1.4. Necesidad de la Tesis

Inicialmente esta tesis surge de la observación de la tendencia en la evolución tecnológica de las tarjetas inteligentes actuales hacia dispositivos en red y la correlación existente respecto a los terminales y redes de acceso; por ello nuestro trabajo se detiene en el consecuente impacto sobre los procesos de autenticación remota que podrían verse involucrados.

Un necesario análisis sobre la orientación *tradicional* en el diseño de protocolos de autenticación para tarjetas inteligentes, nos mostrará cómo han sido incluidas en el esquema de autenticación como un dispositivo de soporte (*token hardware*), en lugar de un dispositivo con entidad propia dentro del sistema. De esta manera, en este trabajo destacamos la inexistencia hasta el momento de propuestas robustas que rompan con ese enfoque tradicional e incorporen la autenticación mutua remota de la tarjeta inteligente como cualquier otro dispositivo en red. Este proceso debería llevarse a cabo de forma independiente del terminal y garantizando en todo momento la interoperabilidad mediante protocolos estandarizados, permitiendo la migración suave -al tiempo que es computacionalmente sostenible-, de los actuales procedimientos de autenticación diseñados específicamente para tarjetas ISO 7816, hacia la aplicación de dichos procedimientos hacia entornos de tarjetas en red, en tanto que esta tecnología se consolida definitivamente.

Así, esta tesis pretende cubrir un hueco en el panorama de investigación, ante la inexistencia de trabajos previos que contemplen el problema de la autenticación remota de la tarjeta inteligente de una forma global; que dé cabida al conjunto de convergencias tecnológicas (dispositivos y redes de acceso) previstas por tratarse de un escenario factible a medio/largo plazo, y por ello parte hacia la búsqueda de un *Marco de Referencia* que sirva como base de estudio y motor de soluciones aplicables, en términos de una arquitectura de protocolos de autenticación, que plasme las particularidades de esta circunstancia.

1.5. Objetivos de la Tesis

En este punto, se pretende establecer un conjunto de objetivos parciales que finalmente culminen en dos, que pueden ser considerados principales; el primero de los cuales consistiría en alcanzar el mencionado Marco de Referencia que tendría cabida bajo el epígrafe: *"Marco de Autenticación para Tarjetas Inteligentes en Red"*, que deberá responder a las necesidades presentadas en la sección anterior. El segundo de los objetivos principales será aplicar dicho Marco de Autenticación a un escenario concreto en aras de demostrar su viabilidad y sentido práctico.

Se detallan a continuación los objetivos parciales planteados para la correcta realización de esta tesis:

- Análisis del enfoque tradicional en el diseño de protocolos de autenticación con tarjetas inteligentes, que permitirá identificar un nuevo enfoque en tal diseño con el objeto de afrontar las necesidades que las nuevas tendencias en esta tecnología están demandando.

- Estudio de la evolución que se está produciendo en las redes locales inalámbricas, como firmes candidatas a servir *redes de acceso* ante dispositivos, entre los que se incluye la tarjeta inteligente, solicitante de servicios de autenticación.

- Como resultado de los análisis y estudios anteriores, esta tesis aspira a definir un nuevo modelo de autenticación remota que sirva de referencia para el estudio y diseño de arquitecturas de protocolos de autenticación en las que las tarjetas inteligentes queden contempladas desde las primeras fases de diseño como *host* común integrado en la infraestructura de red. Para ello se prevé la necesidad de ciertos requisitos de autenticación asociados a dicho modelo para establecer su dimensión y acotaciones de seguridad correspondientes.

- Análisis de la seguridad del modelo a partir de las relaciones de confianza entre las entidades participantes, que permita garantizar un proceso de autenticación robusto y seguro.

- Se plantea en este trabajo el objetivo de especificar una arquitectura de protocolos de autenticación para tarjetas inteligentes basada en el modelo anterior, que sirva de enlace entre lo conceptual y la implementación práctica en un escenario concreto. No se descarta en el ajuste de esta arquitectura, una redefinición de la aplicación de ciertos protocolos en la tarjeta inteligente, de forma que permita una integración de ésta en el sentido requerido por el modelo de autenticación remota.

- En definitiva, este conjunto de modelos, requisitos y arquitectura conformarán el pretendido nuevo *Marco de Autenticación para Tarjetas Inteligentes en Red*.

- El diseño e implementación de protocolos de la arquitectura necesarios y la prueba de las funcionalidades esperadas en la tarjeta inteligente para su correcta integración, conforman una de las últimas fases de esta tesis y quedará detallada en el presente documento.

- Finalmente, como aplicación práctica del *Marco de Autenticación* resultante, se describe su empleo sobre un escenario realista de pago electrónico con tarjetas inteligentes, destacando su versatilidad y contribución al proceso de migración hacia la nueva generación de tarjetas inteligentes.

1.6. Organización de la Memoria

La presente memoria se organiza de la siguiente manera. Tras el presente capítulo de introducción, en el Capítulo 2 se detallan el estudio y análisis que han cimentado los antecedentes de esta tesis, así como los avances en el área de la seguridad de tarjetas inteligentes y tecnologías relacionadas en el contexto de este trabajo, y que conforman un sólido estado de la cuestión en estas materias.

El Capítulo 3, se centra en la descripción del *Marco de Autenticación para Tarjetas Inteligentes en Red* que incluirá, tras el análisis previo, la descripción de los modelos, requisitos y arquitectura de autenticación desarrollados en el transcurso de esta tesis.

En el Capítulo 4, se trata el diseño e implementación del modelo y protocolos que afecta a la tarjeta inteligente, para en el Capítulo 5 proceder con las pruebas de las funcionalidades esperadas en ésta una vez finalizada la implementación. Un conjunto de tests, con tal objetivo, se verán descritos en dicho capítulo.

En el Capítulo 6, con el fin de dar respuesta al segundo de los objetivos principales, se describe detalladamente la aplicación del Marco de Autenticación propuesto en este trabajo a un escenario realista, dando cuenta de su espíritu de practicidad y utilidad. El escenario ha sido identificado a partir del estudio de las tendencias tecnológicas que planean sobre este área de trabajo: *"pago electrónico con tarjetas inteligentes en entornos inalámbricos"*. Finalmente, las Conclusiones del Capítulo 7 y la Bibliografía completan esta tesis.

Capítulo 2.

Antecedentes y Estado de la Cuestión

2. Antecedentes y Estado de la Cuestión

2.1. Antecedentes

En las siguientes secciones, se realizan las consideraciones y análisis previos que permiten conocer en mayor profundidad las peculiaridades que vienen definiendo los protocolos de autenticación con tarjetas inteligentes, y que sirven como punto de partida; de cuestionamiento, por un lado, y elemento dinamizador del planteamiento de nuestro trabajo, por otro. Esta primera parte de antecedentes dará paso en el punto 2.2 al estado de la cuestión sobre el que se cimienta esta tesis.

2.1.1. Diseño de Protocolos de Autenticación en Tarjetas Inteligentes

En nuestra opinión, el enfoque histórico en el diseño de protocolos de autenticación en tarjetas inteligentes ha quedado marcado por la naturaleza de la comunicación de este dispositivo con el resto del sistema, altamente dependiente del terminal o *host*. Por tanto, la tarjeta ha sido vista más como un elemento de soporte al servicio del usuario, que como una entidad autónoma y con capacidad de comunicarse con el sistema de forma segura. A continuación, realizamos algunas consideraciones que ponen de manifiesto este hecho.

Almacén de información. Históricamente las tarjetas empleadas en multitud de aplicaciones han sido las de banda magnética, de uso masivo en servicios de banca y financieros, comportándose como meros elementos de almacén de información inseguros. Desde las primeras tarjetas inteligentes de memoria, ampliamente desplegadas en entornos corporativos (control de acceso, micro-pago en máquinas, etc.) y como tarjetas telefónicas, ya se pretendió avanzar en seguridad del almacenamiento, dadas las ventajas, que en este sentido, podían aportar. Las modernas tarjetas inteligentes, aún cuando mejoraban su capacidad de procesado incluido el criptográfico, en buena medida han continuado esa inercia. Por ello, el diseño de los primeros protocolos de autenticación en estas tarjetas incidía netamente en su capacidad de soporte portátil de ciertos credenciales de seguridad (identificador, PIN, contraseñas, etc.) asociados al usuario, siendo éste el que debe demostrar su autenticidad frente al sistema. Bajo este enfoque, en estos protocolos de autenticación la comunicación con el sistema al que se pretende acceder es nula o prácticamente nula, quedando restringida a una comunicación local entre el portador de la tarjeta y la misma, interviniendo como intermediario el terminal lector. El transporte del protocolo de autenticación por tanto se diseña sobre las especificaciones ISO 7816.

Rol de Servidor. Típicamente el diseño de protocolos de autenticación con tarjetas inteligentes ha quedado también condicionado por el hecho que supone actuar en el rol de servidor, como única posibilidad de comunicación con el sistema y participando el terminal en el rol de cliente. Por tanto, ha sido un dispositivo muy limitado en este sentido, al depender notablemente de dicho terminal, quedando empobrecida la comunicación, incluido el transporte de los mensajes de autenticación, por la funcionalidad *push,* comandada desde éste. Con el advenimiento de técnicas más modernas, como la tecnología basada en OTA (over-the-air) [SAT06] aplicable en entornos de telefonía móvil, se consiguió incorporar el rol de cliente y cierta

proactividad en la tarjeta inteligente (además de incluir la emisión comandos de forma remota [3G-31116]), pero hasta el momento esta funcionalidad queda restringida a las módulos SIM, insertados en las estaciones móviles.

Marcas de tiempo. Otro condicionante histórico en el diseño de protocolos de autenticación con tarjetas inteligentes ha sido la imposibilidad de emplear marcas de tiempo (time-stamp) que a menudo son requeridas en éstos para garantizar la frescura de ciertos mensajes. El concepto de time-stamp fue inicialmente explotado en los criptosistemas basados en identidad [Sha84] y en algoritmos de firma digital como el ElGamal [ElG85] cuya implicación en esquemas más recientes ha sido muy importante. Sin embargo, no siempre es posible extender la utilización de time-stamps a cualquier esquema, especialmente cuando se trata de procesos de autenticación con tarjetas inteligentes. Como es ampliamente conocido, éstas no disponen de reloj interno dada la ausencia de una batería propia. La tarjeta inteligente recibe su alimentación del dispositivo de lectura y, por tanto, el *tick* interno de la tarjeta depende netamente del *host*. Así mismo, la noción de un valor del tiempo universal o similar sólo sería posible si el lector suministra dicho valor en nombre de la tarjeta. Obviamente, esta íntima dependencia en el uso de *time-stamp* hace de ésta una técnica altamente desconfiable y por tanto no es recomendable su utilización en las autenticación con tarjetas inteligentes. Es fácil pensar en un escenario en el que el usuario debe insertar su tarjeta en un dispositivo desconocido y público. Pese a algunos desafortunados intentos, los protocolos de autenticación en tarjetas inteligentes han recurrido mayoritariamente a la utilización de *nonces*.

Autenticación simple. La concepción inicial de la autenticación entre entidades dentro de un entorno de red, como uno de los servicios básicos de la seguridad, lleva siempre aparejada la posibilidad de que esta autenticación sea recíproca entre las entidades que participan en el proceso y, por tanto, se dote de robustez al sistema maximizando las garantías de seguridad. Son bien conocidos distintos protocolos que hacen posible esta mutua autenticación, sin embargo, a menudo cuestiones que tenían que ver más con el coste de implementación (coste computacional o coste de implantación masiva) que con la existencia de soluciones efectivas hicieron que en la mayoría de los casos de escenarios reales con tarjetas inteligentes se implementara un protocolo de autenticación simple en la que, como queda dicho, la tarjeta hacía las veces de servidor. Aunque técnicas posteriores permiten una autenticación mutua, en muy pocos casos el proceso de autenticación lo inicia de forma activa la propia tarjeta, dependiendo para ello de nuevo del terminal y por tanto carente de la pretendida autonomía.

Pila de protocolos ISO 7816. Siendo este estándar la propia esencia de una tarjeta inteligente, sus peculiaridades han hecho que el diseño de protocolos de autenticación sean específicos para estos dispositivos. El resultado son protocolos difícilmente interoparables en el entorno de red, posicionándose así frente a un diseño universal que garantiza su conexión con un mundo todo-IP, como máxima de diseño para cualquier sistema de comunicación y de seguridad. Si bien es cierto que, bajo ciertas técnicas de adaptación, se puede conseguir en muchos casos dicha interoperabilidad, no todos los protocolos de autenticación diseñados para sistemas de redes, se ajustan convenientemente al entorno de la tarjeta inteligente y viceversa. Especial atención ha de prestarse en este sentido, en cuanto al transporte de los mensajes de autenticación y al papel de dependencia del terminal en dicho proceso. De otro lado, un diseño excesivamente particular puede fácilmente quebrar el sentido y la robustez de cualquier

protocolo ante la celeridad con la que se producen los avances tecnológicos, normalmente encaminados a conseguir un elevado grado de integración e interoperabilidad. Como prueba de ello, y ya introducido en esta tesis, cada vez se hace más patente las directrices de investigación y desarrollo que apuntan hacia una tarjeta inteligente en red bajo la etiqueta TCP/IP frente al actual modelo ISO 7816.

Autenticación remota. El conjunto de los aspectos señalados podría justificar la práctica inexistencia de protocolos de autenticación remota. Si bien para los procesos de autenticación local la tarjeta se comporta como cualquier otro dispositivo con un interfaz de comunicación particular, para la autenticación remota adolece de las carencias que se derivan de las características anteriores. En este tipo de procesos, la dependencia del terminal es latente, no sólo en lo referido a la comunicación con la entidad remota en el entorno de red, sino especialmente en el plano de la autenticación, dificultando por tanto la posibilidad de integrar la tarjeta inteligente en la red, de forma transparente. Así, como parte de los antecedentes que fundamentan esta tesis, dedicamos un espacio en nuestro trabajo al análisis de esta circunstancia en la próxima sección.

2.1.2. Análisis de la Autenticación Remota de la Tarjeta Inteligente según la Atomicidad del diseño

Según se explicaba en el epígrafe anterior hay aspectos propios de la naturaleza de la tecnología de tarjetas inteligentes, que han determinado en gran parte la manera en la que tradicionalmente los protocolos de autenticación se han diseñado con este, o para este, tipo de dispositivos. La ausencia de autonomía que se deriva de esas características se ve especialmente repercutida en el diseño de los protocolos de autenticación remota, que carecen de la consecuente atomicidad, significativamente necesaria cuando alguno de los dispositivos con los que se comparte las funcionalidades de autenticación pueden calificarse de *no confiables*. En el caso que nos ocupa, tal dispositivo podría ser el terminal, pudiendo verse cuestionado en este caso los principios básicos de seguridad. Es clara, por tanto, la necesidad de ahondar en el estudio de los procesos de autenticación para conseguir la integración de la tarjeta inteligente como un dispositivo en red que incorpore de forma atómica dicha funcionalidad. En el presente apartado, se procede con el análisis que se centra en identificar: en qué medida el protocolo de autenticación remota se diseña e implementa de forma atómica y en la conveniencia de hacerlo así.

El diseño de multitud de protocolos de seguridad en general, y de autenticación remota en particular, no reparan en la atomicidad del diseño cuando se trata de tarjetas inteligentes; de esta manera, dan por sentado que la funcionalidad de solicitante de autenticación queda repartida entre tarjeta inteligente y terminal (*split supplicant*), como si se tratara de una única entidad en cuanto autenticación se refiere.

Un claro ejemplo de esta circunstancia es el referido a la asociación de un teléfono móvil, MS, a una red GPRS [3G-23060]. Aquí, la tarjeta SIM participa como elemento de soporte al MS en el proceso de autenticación remota. Este *soporte* de la tarjeta se basa en el almacenamiento de unos credenciales de seguridad y la ejecución del

algoritmo criptográfico oportuno [3G-43020][4]. Por otro lado, podemos considerar al MS como el dispositivo que facilita la comunicación con el nodo remoto en la red (SGSN) y con el que se intercambiarán los mensajes de autenticación (Figura 2.1). La confianza entre la tarjeta SIM y el terminal MS no se ve cuestionada en este esquema y, más allá, podríamos llegar a afirmar que en realidad se está autenticando a un determinado MS, al que se le permite o deniega el acceso, en lugar de autenticar a la SIM que identifica al abonado. Bajo este esquema, queda claro el papel de soporte de la SIM para autenticar al MS, frente a la versión donde un MS sirviera de soporte para autenticar una tarjeta SIM.

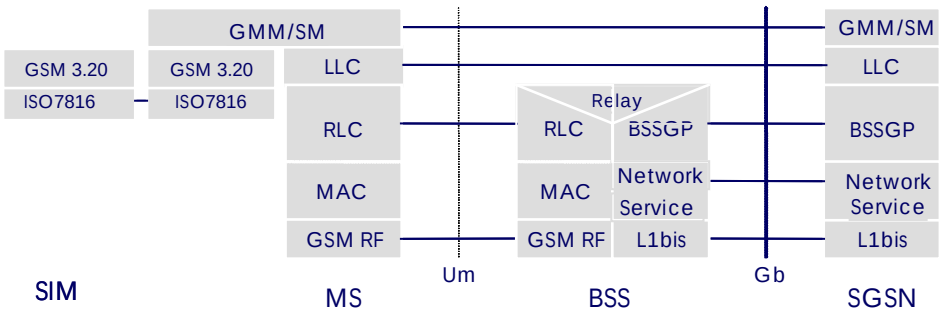

Figura 2.1 Infraestructura de Autenticación de un terminal móvil, MS, en la red GPRS

En el primer caso, SIM y MS son consideradas como una única entidad, desde el plano de la autenticación; en el segundo, podrían considerarse entidades distintas, siempre y cuando, se atendiera a la atomicidad en el diseño del protocolo y mecanismos de autenticación. Aunque el ejemplo presentado, es un claro caso de autenticación remota con tarjeta inteligente en un entorno en red, no estamos en disposición de afirmar que se trata de una tarjeta inteligente *integrada* en la red. La Figura 2.2 modela el estilo *tradicional* en el que se diseñan los protocolos de autenticación remota en tarjetas inteligentes, respecto a la atomicidad, y al que se ajusta el caso descrito.

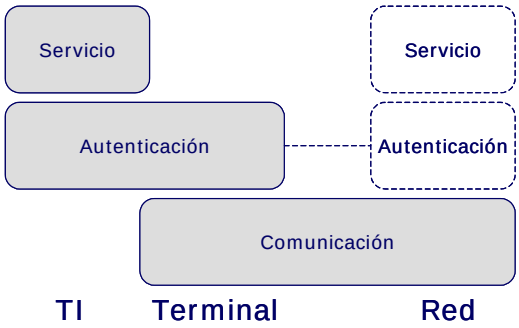

Figura 2.2 Modelo tradicional de los protocolos de autenticación remota de tarjetas inteligentes, según la atomicidad en el diseño

[4] 3GPP TS 43.020 es el estándar actual que desciende de GSM 3.20, comúnmente conocido.

En la parte superior se representa el contexto de “servicio”, en donde hacemos referencia a las aplicaciones o servicios objetivos a los que podría accederse una vez realizada con éxito la autenticación. Obsérvese, que la autenticación puede ser considerada en sí mismo un servicio, aunque es conveniente para un mejor análisis la separación de esta funcionalidad en un contexto diferente (“autenticación”), y que es responsable explícita y netamente de todos los mecanismos involucrados en el proceso de la autenticación. Por último y en la parte inferior de este modelo, aparece un contexto denominado genéricamente “comunicación”, que es el encargado de la conexión, establecer el enlace y transportar los mensajes correspondientes del contexto del plano superior; en definitiva y en nuestro caso, servir de portador de dichos mensajes desde/ hacia la tarjeta inteligente hacia/desde las entidades remotas en el sistema, encargadas de la autenticación y autorización en el acceso.

Como se puede apreciar en el modelo la Figura 2.2, una vez identificada la funcionalidad dividida del solicitante de autenticación (*split-supplicant*), parece razonable evitar un diseño del protocolo de autenticación descuidando el contexto de "comunicación", en tanto que la responsabilidad de comunicación con la red, según este modelo, recae íntegramente en el terminal; es decir, es éste en definitiva el encargado de generar y transportar los mensajes de autenticación hacia/ desde el resto del sistema, implementando los protocolos oportunos (GMM/SM, GPRS Mobility & Session Management, para el ejemplo indicado) que intervienen directamente en la autenticación.

Como ejemplo de atomicidad en el diseño de los protocolos de autenticación para tarjetas inteligentes, podría señalarse el control de acceso físico. En tales circunstancias, la tarjeta y el terminal participan autónoma e inequívocamente con roles separados de solicitante y verificador. Aunque se trata de un caso claramente representativo, se aleja del marco de trabajo que nos ocupa por tratarse de un caso de autenticación local que se realiza sobre el interfaz ISO 7816. En la Figura 2.3, se ilustra un ejemplo de un proceso de autenticación basado en reto-respuesta entre tarjeta y terminal, propio de un caso de control de acceso físico.

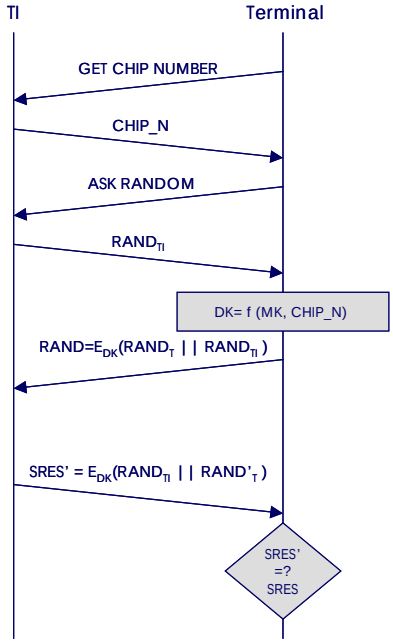

Figura 2.3 Ejemplo de Control de Acceso Físico. El terminal autentica a la tarjeta si comprueba que SRES' = $E_{DK}(RAND'_{TI} || RAND_T)$

Por tanto, este análisis nos lleva a *re*considerar el diseño de protocolos de autenticación remota basados en el modelo representado en la Figura 2.2 por la falta de atomicidad del mismo. Este hecho podría traducirse en una flagrante vulnerabilidad, en escenarios en los que el terminal pudiera calificarse como *no confiable*. Adicionalmente, conviene señalar la repercusión en la comunicación con el sistema. Así, las tarjetas inteligentes con protocolos de autenticación diseñados sobre este modelo, muestran una seria resistencia a la migración hacia otros entornos, como redes TCP/IP, hecho que parece ineludible.

Como conclusión, se hace recomendable un diseño atómico en el que la tarjeta se presente como único elemento en la funcionalidad de solicitante de autenticación y pueda así autenticarse por sí misma (*self-authenticable*), ganando en independencia respecto al terminal, Figura 2.3a. Pero más allá, este hecho le podría permitir, bajo un diseño más orientado al contexto de comunicación, Figura 2.3b, ganar también en autonomía en este plano e incorporar sus propios mecanismos de comunicación acorde con el protocolo de autenticación y con el sistema, y comportándose en cierta medida como un nodo más, facilitando la migración hacia los entornos en red. En el próximo capítulo se profundiza sobre esta perspectiva.

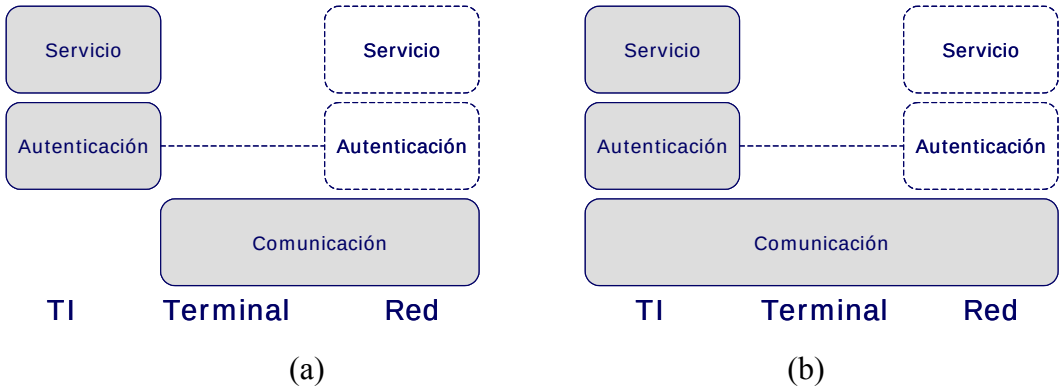

Figura 2.3 (a) Diseño atómico del protocolo de autenticación remota; (b) caso del mismo protocolo pero además orientado al contexto de comunicación.

Para entender en qué manera se ha de producir esta migración, es sin duda necesario conocer qué tendencia se están identificando en las redes de acceso para dispositivos en general, porque de alguna manera estas redes supondrán el primer reto tecnológico al que deberán *enfrentarse* las tarjetas inteligentes en evolución. En los próximos epígrafes se ahonda en esta materia.

2.1.3. Tendencia en la tecnología de redes de acceso y sus protocolos de autenticación

En este apartado se ha procedido con el estudio de una de las claras tendencias en las tecnologías de acceso a redes. Este aspecto resulta especialmente significativo para entender en qué contexto se producirá la integración de las tarjetas inteligentes según dicha tendencia y que marcará, indudablemente, un referente a observar en el desarrollo de esta tecnología, y por tanto de los esquemas de autenticación de la tarjeta que tengan cabida.

Como primera aproximación, se parte de una arquitectura genérica aplicable a una diversidad de entornos, y en la que la tarjeta inteligente adquiere entidad propia, Figura 2.4. Obsérvese, la coexistencia de una red pública como Internet junto con líneas y redes de infraestructura bajo el control administrativo de operadores privados para la provisión de servicios de distinta índole.

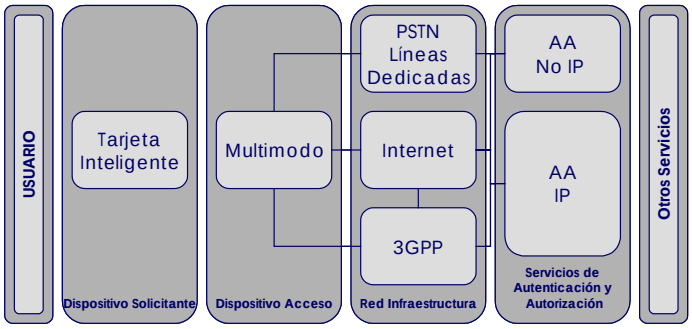

Figura 2.4 Tarjeta Inteligente en la arquitectura genérica

En este esquema el usuario es la persona física que previo registro, normalmente contractual, dispone de una tarjeta personalizada emitida por la correspondiente entidad que velará por la autenticación y autorización de sus accesos u operaciones y potencialmente podrá facilitarle una variedad de servicios adicionales.

La tarjeta inteligente, que almacena los credenciales oportunos de dicho usuario y opera en el entorno de lo electrónico en su nombre, no sólo es el elemento que le identifica sino que se convierte en el dispositivo autónomo que interacciona directamente con el sistema y por tanto en el solicitante de los servicios de autenticación y autorización. Según el esquema de autenticación llevado a cabo, dicha tarjeta podrá autenticar también a la entidad remota que ofrece el servicio e incluso firmar digitalmente ciertas operaciones, con el fortalecimiento del no repudio del proceso.

Como punto de partida de nuestro trabajo, consideraremos un dispositivo de acceso multimodo, que además de disponer del correspondiente lector de tarjeta inteligente y una variedad de interfaces de usuario, permite la conexión con los servicios de autenticación y autorización, a través de líneas dedicadas, normalmente contratadas a operadores de telefonía fija haciendo uso de su red pública conmutada de telefonía (PSTN), Internet o mediante una conexión inalámbrica a través de operadores de redes de telefonía móvil de tercera generación (3G).

No obstante, a partir de esta clasificación en las redes de infraestructura, otras variantes de interconexión son posibles (p.e. 3GPP/Internet/Red Corporativa). Dependiendo de la criticidad del sistema y de las medidas adicionales de seguridad implementadas, estas opciones deberían ser reconsideradas.

En cuanto al dominio de los servicios de autenticación y autorización, ha señalarse que estos corresponden a las entidades que tienen potestad sobre otros servicios finales a ofrecer. Por tanto, conviene distinguir inicialmente dichos procesos de autenticación para el acceso a las redes de infraestructura, normalmente operados por los correspondientes proveedores, de los servicios de autenticación para el acceso a otros finales, ofertados por entidades de distinta índole. En el esquema representado en la Figura 2.4, se ha realizado esta diferenciación; dichos servicios finales serán tratados tangencialmente en esta tesis. En principio, los protocolos de autenticación a

implementar pueden ser tanto propietarios y específicos de cada servicio o entidad, como estandarizados y públicos para su integración global.

Aún cuando la interconexión e integración de nuevas tecnologías, como es el caso del acceso inalámbrico (redes locales inalámbricas), se ha producido y se sigue produciendo de forma transparente, la inclusión de las tarjetas inteligentes en estos escenarios ha sido más desde la perspectiva de un dispositivo de activación, que de un dispositivo de red. En tal caso, su comportamiento en cuanto a procedimientos de autenticación se refiere, debería asemejarse, en la medida de lo posible, a un nodo o *host* en un entorno heterogéneo de redes.

Redes de Área Local Inalámbrica como Red de Acceso

En este apartado, se deja constancia del papel fundamental que están jugando, y van a jugar las redes locales, y en concreto las inalámbricas, como redes de acceso de públicas para una multitud de dispositivos y, entre ellos, las tarjetas inteligentes. De esta manera, estos dispositivos no sólo tendrán que adaptarse en gran medida a esta circunstancia sino que además, y desde nuestra óptica, deberán tomar ventaja de ello para establecer mecanismos de autenticación más robustos.

A continuación analizamos cómo, desde nuestra perspectiva, la tecnología de redes locales presenta ciertas características que la hacen merecedora de su sólida consideración como la más adecuada *red de acceso* para la tarjeta inteligente y su pretendida integración como una entidad más en el esquema global de red.

- de forma sintetizada, una *red local* cableada o inalámbrica es una red en capa 2 según el Modelo de Referencia OSI. Esto permitiría una integración de la tarjeta inteligente en la red para la dotación de ciertos servicios, con una pila de protocolos más ligera, sin necesidad de implementar protocolos de red (capa 3) para acceder a éstos.
- los mecanismos y recursos en esta capa 2, tanto en el plano de la comunicación remota como en el de la seguridad, podrían ser lo suficientemente robustos como implementar un adecuado ***servicio de autenticación*** entre dispositivos.
- cualquier solución adoptada en esta dirección, sobre la base de protocolos estandarizados, no excluye la posibilidad de la implementación de otros de capas superiores, cuando así fuese requerido.
- uno los primeros avances en las tarjetas inteligentes en red, según la literatura (ver epígrafe 2.2.3), han ido encaminados hacia la provisión de una capa 2 tipo *Ethernet* en las actuales tarjetas inteligentes ISO 7816.
- la **dependencia** de un terminal de acceso público bajo la etiqueta a priori de *no confiable*, que hasta ahora ha sido ineludible, tras una adecuada reconsideración sobre el papel de éste como dispositivo de la red local de acceso, abriría una interesante línea de trabajo.

Redes de Área Local Inalámbricas Públicas o PWLAN

La interconexión de las redes de área local inalámbrica y redes de telefonía de tercera generación, 3G, (Figura 2.5) es un tendencia tecnológica en la infraestructura de acceso público, *PWLAN* (*Public Wireless LAN*), que viene experimentándose en los últimos años, y cuya consolidación avanza a un ritmo prometedor. A juicio de los expertos, la arquitectura de red que proporciona la integración 3G/WLAN, así como los trabajos e investigaciones que la toman como referencia y ahondan en su estudio, deben ser considerados, junto a otros, como un paso más en el camino que conduce hacia la nueva generación de redes all-IP inalámbricas o de cuarta generación, 4G.

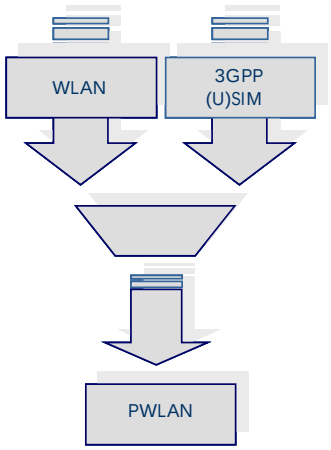

Figura 2.5 Evolución hacia las PWLAN o redes 4G

Las Redes de Área Local Inalámbricas (Wireless Local Area Network o WLAN) como tales, han experimentado un crecimiento sustantivo. El éxito de Internet y la disponibilidad de dispositivos portátiles de precio asequible para el usuario común, provistos de tarjetas inalámbricas con tecnología depurada, ha hecho extensiva la demanda de puntos de acceso inalámbricos a la información digital y a los servicios disponibles a través de la gran red. En el proceso de estandarización de las especificaciones relativas a las redes inalámbricas locales, vienen desarrollándose dos propuestas relevantes: IEEE 802.11 y HiperLAN. Si bien es cierto que, la primera de ellas a copado el interés del mercado, así como, el de los trabajos de investigación y de la industria afines. HiperLAN ha pretendido presentarse como una alternativa a las redes inalámbricas locales desde el sector de las telecomunicaciones europeo, estandarizado por la ETSI (European Telecommunications Standards Institute).

Aunque inicialmente fueron concebidas como una extensión de las redes de área local de tipo corporativo, las WLAN han ido incrementando su popularidad hasta convertirse en redes de acceso para la conectividad IP en ambientes residenciales, entornos SOHO (small office- home office), campus, etc. Más recientemente, los puntos de acceso públicos de gran demanda (hotspots) han proliferado de forma exponencial, permitiendo

así el trasiego de la información digital entre un variado conjunto de entornos, haciéndola accesible casi en todo momento; casi en todo lugar.

Por su parte, los sistemas móviles de tercera generación (3G) son presentados como una solución competitiva para ofrecer servicios, en términos de rendimiento, coste efectivo y variedad de contenidos, entre los que podríamos encontrar aplicaciones multimedia. El proyecto 3GPP (Third Generation Partnership Project) es una iniciativa conjunta de las organizaciones de estandarización de Europa, Japón, EE.UU. y Korea para desarrollar las especificaciones de UMTS (Universal Mobile Telecommunication System). 3GPP fue inicialmente formado para realizar un conjunto común de especificaciones para el sistema de telefonía móvil 3G en armonía para las regiones participantes.

Otros atributos a resaltar en dichos sistemas, serían el amplia área geográfica de cobertura que permiten, con importantes ratios de fiabilidad, y una alta movilidad con *roamings* transparentes y efectivos. Sin embargo, el coste de las licencias de las frecuencias radioeléctricas y la configuración del sistema, para llegar a ofrecer esta cobertura casi ubicua, ha obligado y obliga a los operadores de telefonía móvil a promover grandes inversiones en el despliegue de estas redes de tercera generación.

La competencia frente a la complementariedad entre los sistemas WLAN y 3G ha sido a menudo objeto de cuestionamiento en los centros de investigación y en la industria. Es claro que cada tecnología tiene su nicho en el mercado pero, observando sus características, es fácil comprender el efecto de complemento que la una supone para la otra. Si bien es cierto que las redes inalámbricas locales pueden dar cobertura sólo a pequeñas áreas y permiten una movilidad limitada, su tasa de transmisión de datos podría ser hasta casi treinta veces mayor que la que ofrecen los sistemas 3G. Por tanto, las características de WLAN permiten dar servicios a zonas de gran demanda con altas tasas de transmisión en las que la movilidad no es un requisito. De otro lado, los sistemas 3G, con su soporte de servicios de voz bien establecidos, amplia cobertura y menor tasa de transmisión de datos, son más adecuados para áreas con moderada o baja densidad de demanda, pero con alta movilidad. Adicionalmente, estos sistemas ofrecen una robusta infraestructura de red y de gestión para acometer exigentes requisitos de seguridad, facturación y *roaming*, siendo este último aspecto el que permitiría hablar de las redes inalámbricas locales públicas (Public WLAN o PWLAN), en su máxima expresión [Leu06]. La tendencia en el número de usuarios, representado en la Figura 2.6, refuerzan la inercia de esta convergencia identificada.

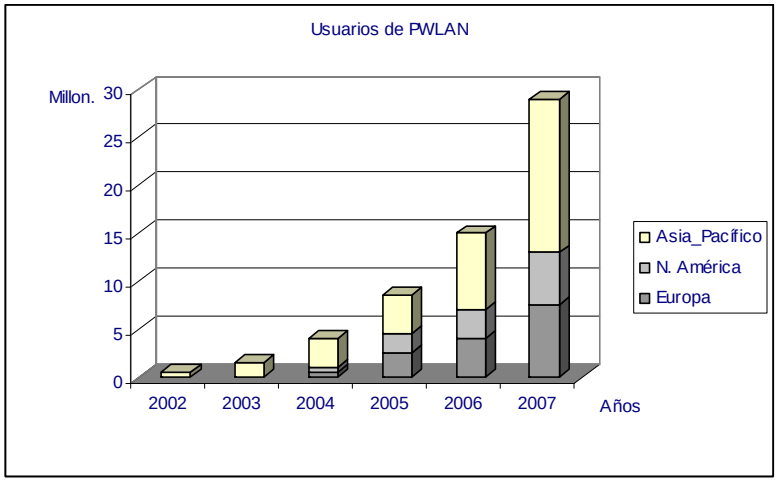

Figura 2.6 Evolución del uso de Redes Locales Inalámbricas Públicas (Fuente: Strategy Analytics)

Así, la integración de los sistemas de telefonía móvil de 3G y las redes inalámbricas locales (también a veces denominada I-WLAN), aunando las ventajas de ambas tecnologías, puede tener un efecto significativo en el desarrollo de servicios que requieran de una alta tasa de transmisión (p.e. servicios multimedia basados en IP, IMS), al tiempo que se dota al sistema de alta movilidad; preservando en todo momento la calidad del servicio ofrecido a una, cada vez mayor, población de usuarios de distinto perfil. En la Tabla 2.1, se muestran resumidamente los puntos en los que ambas tecnologías se complementan, ofreciendo en conjunto una sólida solución.

	3G	WLAN
Penetración	*Buena*	*Mala*
Cobertura	*Amplia*	*Reducida*
Seguridad	*Fuerte*	*Débil*
Ratio Transmisión	*Bajo*	*Alto*
Coste Implantación	*Alto*	*Bajo*
Tasa Licencia	*Muy Alta*	*No requiere*
Construcción	*Difícil*	*Fácil*
Soporte a la Movilidad	*Alto*	*Pobre*

Tabla 2.1 Comparativa de las propiedades de las redes WLAN y de 3GPP

De esta manera, es necesario hablar de un terminal multimodo 3G/WLAN capaz de acceder a servicios particulares ofrecidos por cada sistema, pero más allá, la integración 3G/WLAN proporcionaría soluciones efectivas de multiacceso; es decir, soluciones integrales que aporten movilidad transparente entre las distintas tecnologías de acceso, permitiendo la continuidad de una sesión iniciada. Los dispositivos portátiles de nueva

generación de tipo PDA, representan una solución efectiva como materialización de este tipo de terminales multimodo, que implementan sólidos mecanismos de seguridad. Su evolución en el mercado, ilustrada en la Figura 2.7 confirma esta tendencia.

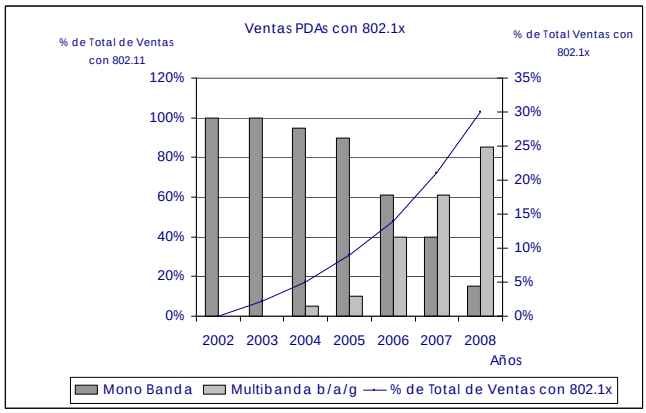

Figura 2.7 Evolución de uso de PDAs como terminales seguros multibanda (Fuente: Strategy Analytics)

Por tanto, desde nuestro enfoque conviene revisar el esquema representado en el comienzo de este epígrafe (Figura 2.1) que atendía a una visión descriptiva, tanto de las tecnologías tradicionales como de las más recientes, pero ajeno en cierta manera de las posibles tendencias en la red (o infraestructura) de acceso que, en los próximos años, pudieran moldear esta categorización de alto nivel hacia otras direcciones. Según esta tendencia, dicho esquema debería evolucionar hacia el representado en la Figura 2.8, que redefinirá un conjunto de potenciales escenarios con múltiples aplicaciones, y en donde la tarjeta inteligente participa de actor principal.

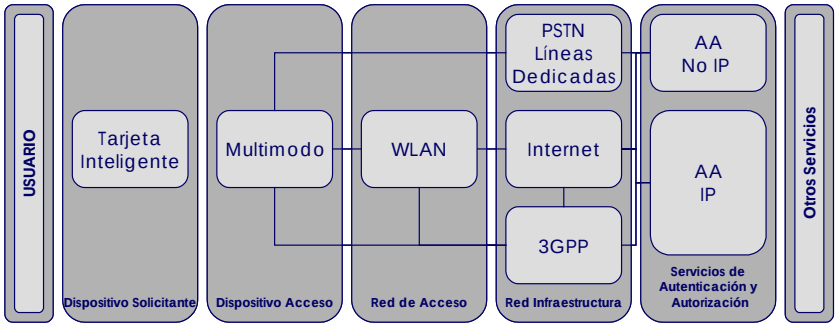

Figura 2.8 Tarjeta Inteligente en una arquitectura evolucionada

En cuanto al plano de los protocolos de autenticación del dispositivo de acceso en estos escenarios, se está experimentando consecuentemente una migración suave desde los mecanismos basados en (U)SIM en entornos de 3GPP (que se autentican finalmente contra bases y registros de abonados, HLR/HSS) y de los basados en EAPoL (802.1X/EAP) que incluyen tecnologías como RADIUS [Rig00][Abo03] o DIAMETER [Ero05], típicos en redes locales inalámbricas, hacia soluciones denominadas "basadas en SIM" (*SIM-based*) que enmarcan protocolos tales como EAP-SIM [Hav06], EAP-AKA [Ark06]. Estos protocolos, recientemente estandarizados, permiten llevar a cabo una autenticación mutua entre el terminal inalámbrico y el servidor de acceso. De un lado, los usuarios de dispositivos móviles, cada vez más, están acostumbrados a la existencia y necesidad de una tarjeta SIM que le permite como abonado el acceso a un conjunto de servicios a través de su dispositivo móvil; de otro lado, los operadores de estas redes no requieren de una credencial distinta a las tarjetas SIM para facturar los servicios adicionales ofrecidos a través de las PWLAN a tales abonados. Los esquemas de autenticación basados en SIM, se presentan como alternativa a los esquemas "basados en Web" (Web-based) e incluso redes privadas virtuales, RPV.

En la actualidad, la mayoría de los operadores de WLAN públicas (PWLAN) hacen uso del denominado Método de Acceso Universal basado en Web (Web-based universal access method) para los procesos de autenticación, el cual está también recomendado como la mejor de las actuales prácticas para el *roaming* entre operadores según la Wi-Fi Alliance [WI-FI]. La autenticación basada en Web sin certificado de cliente está comúnmente extendida y es de fácil implementación en la mayoría de los sistemas PWLAN. Sin embargo, balancear las exigencias de la demanda frente a unos requisitos de seguridad razonables no es siempre una cuestión trivial. Así, mientras los esquemas de autenticación basados en Web carecen de una relación de confianza (autenticación) bi-direccional entre el usuario (dispositivo) y el servidor de autenticación, los procedimientos de autenticación basados en SIM van adquiriendo mayor relevancia, y se presentan como una sólida tendencia.

Este hecho, por tanto, nos obliga a considerar la posibilidad de hacer operar las tarjetas inteligentes sobre este tipo de redes de acceso emergentes, que abren un nuevo espectro de posibilidades desde el punto de vista tecnológico, así como desde los potenciales modelos de negocio. Así mismo, las consideraciones relativas a la autenticación remota de estas tarjetas en este contexto concreto se hacen imprescindibles en una parcela no lo suficientemente explorada. La carencia de un modelo de referencia global que integre la tarjeta en el sistema de red de forma coherente con la evolución en la que ambas tecnologías se ven inmersas, completa el origen de la problemática de la que se ocupa la presente tesis, y en cuyo proceso de madurez pretende contribuir.

No cabe duda de que los avances desarrollados en seguridad de las redes de acceso basadas en la interconexión 3G/WLAN o PWLAN, así como en la seguridad de las tarjetas inteligentes, han sido múltiples y se han producido a un ritmo significativo. El conocimiento de un estado de la cuestión de éstos nos permitirá enfocar de la forma más coherente la problemática identificada.

2.2. Estado de la Cuestión

2.2.1. Criptografía en Tarjetas Inteligentes

Los dos pilares iniciales de seguridad que propiciaron el despliegue masivo de las tarjetas inteligentes tuvieron que ver con el hardware, al ser idealizados desde los comienzos como dispositivos herméticos muy resistentes a su manipulación, por un lado, y por tener la capacidad de implementar a muy bajo nivel, eficientes funcionalidades criptográficas, por otro. Casi en los albores de la tecnología, los expertos se cuestionaban si tales características podrían desmerecer el potencial de ciertos algoritmos criptográficos [Des87] o los esfuerzos para combatir las restricciones computacionales propias de estos dispositivos al implementar mecanismos de clave pública [Sha95]; sin embargo, estudios más exhaustivos y el avance de las tecnologías, también para los *hackers*, ponían la voz de alarma sobre las vulnerabilidades de la implementación física de los criptosistemas (conocidos como ataques *side-channel*) que presentaban estos dispositivos, así como los derivados de la manipulación física de la propia tarjeta [And96][And97]. Después de lo cual fue necesaria una reflexión sobre la verdadera capacidad y resistencia de las tarjetas inteligentes como elementos robustos de seguridad, señalándose la necesidad de un proceso de madurez pendiente en torno a esta tecnología [Qui97]. Este proceso vendría reforzado tanto por los pasos dados en la implementación de algoritmos de cifrado en bloque más robustos -los candidatos a AES Twofish y Serpent [Sch98][And98]-, como por los avances en la fabricación de chips criptográficos. Estos primeros criptoprocesadores, [Han98][Köm99], permitían implementar algoritmos de clave pública con cierta eficiencia y, en sucesivos años, se mejorarían las características del hardware suplementario con funciones de seguridad [Tri01]; más recientemente, el refinamiento de las soluciones hardware, como complemento a los algoritmos criptográficos (p.e. en la mejora de la generación de números realmente aleatorios [Buc03]) favorecían la definición de las tarjetas inteligentes como dispositivos altamente seguros.

Por otro lado y mientras tanto, a finales de la década de los noventa, no se había bajado la guardia en la búsqueda de contramedidas en prevención de ataques de tipo *side-channel*. Así, contra las técnicas de análisis en términos de potencia publicadas por Kocher [Koc99] o un poco más tarde con técnicas más sofisticadas [Sko03], no dejaron de publicarse trabajos orientados a la protección contra dichos ataques, basados en los defectos o fenómenos físicos inherentes a las operaciones criptográficas realizadas por el hardware de las tarjetas inteligentes [Sha00] [Qui01] [Moo02]. A éstas, acompañaban también técnicas basadas en el tratamiento interno de los datos (*data scrambling*) con el objeto de dificultar su captura en un posible ataque [Bri01]. No obstante, y desafortunadamente, estos dispositivos no permanecen ajenos a posibles ataques bajo técnicas más recientes basadas en DPA [Osw06].

Pueden considerarse los primeros años de la presente década, como el inicio de la madurez de las tarjetas inteligentes criptográficas [Gui01] [Bor01] en las que la implementación de robustos algoritmos de autenticación empezaban a destacar.

2.2.2. Taxonomía de los Protocolos de Autenticación Remota con Tarjetas Inteligentes

En este apartado se pretende llevar a cabo una taxonomía de las protocolos de autenticación aplicada a tarjetas inteligentes. Como referencia se ha tomado los criterios y clasificaciones señalados en la Guía de Autenticación On-line [NIST 800-63] editada por el Instituto Nacional de Estándares y Tecnologías del Departamento de Comercio del gobierno de Estados Unidos (National Institute of Standards and Technology, NIST). Según esta guía, la aplicación de tarjetas inteligentes en una correcta implementación de un protocolo de autenticación le garantizaría el máximo nivel de prestaciones de seguridad (Nivel 4). Dicho nivel está basado en la Prueba de Posesión (Proof of Possession) de una clave a través de un protocolo criptográfico implementado en un dispositivo hardware conforme a [FIPS 140-2]. Bajo estas premisas la tarjeta inteligente proporciona un método seguro de autenticación, basado en dos factores.

Conviene aclarar que un protocolo basado en la Prueba de Posesión es aquel en el que el demandante (*claimant*) debe probar ante el verificador (*verifier*) que posee y controla -es decir que tiene la capacidad de activar y hacer uso de- un *token* que verifica su identidad (algún elemento de prueba o señal como una clave, una contraseña, etc.), en el protocolo de autenticación.

La clasificación realizada por dicho organismo, Figura 2.9, toma como referencia el enfoque que en cada caso se adopta con respecto a la Prueba de Posesión, PdP, (Proof of Possession, PoP) en el protocolo de autenticación. Tomando como partida este hecho, la guía identifica los siguientes tipos de protocolos de autenticación:

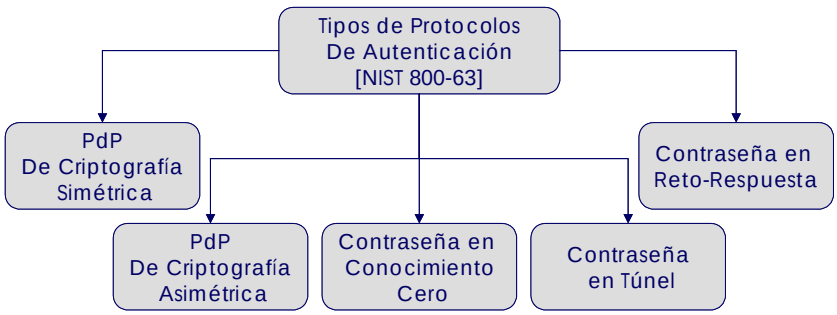

Figura 2.9 Tipos de Protocolos de Autenticación Remota según NIST 800-63

Prueba de Posesión basada en una clave privada. Hace referencia a aquellos protocolos de autenticación basados en criptografía asimétrica y que incluirían infraestructuras de clave pública, en los que técnicas de cifrado y firma digital tendrían cabida. Las aplicaciones como DNI-electrónico o pago electrónico con tarjetas inteligentes EMV (en el caso de autenticación off-line) [EMV04-2] serían buen ejemplo de la utilización de este tipo protocolo de autenticación en estas tarjetas.

Prueba de Posesión basada en clave simétrica. Hace referencia a protocolos de autenticación basados en criptografía simétrica y, por tanto, ambos extremos de la comunicación deberán conocer, o en la mayoría de los casos derivar, una clave sesión con la que podrán cifrar el intercambio de mensajes. La capacidad de conocer o derivar tal clave de sesión da muestras a ambas partes de que la entidad remota es quien dice ser, y por tanto queda autenticada. Esto no excluye que tal clave se utilice para cifrar algún otro *token* (p.e. una contraseña), que añada grados de seguridad al sistema. En aplicaciones de pago electrónico con tarjetas inteligentes EMV [EMV04-2], se hace uso de este esquema de autenticación en el caso de que ésta se produzca de forma remota u *on-line*.

De ambos ejemplos de autenticación con tarjetas inteligentes se dará amplia cuenta a lo largo de esta tesis. A continuación se repasa el estado del arte de los otros tipos de protocolos de autenticación, que aunque de gran interés para la mejor comprensión de nuestro marco de trabajo, no son empleados directamente.

Protocolo de Contraseña en Túnel, es aquel en el que la contraseña es enviada bajo un canal protegido. Como mejor ejemplo, el protocolo TLS. Este protocolo es empleado a menudo con el certificado de clave pública de un verificador para autenticar al demandante, establecer una clave de sesión entre ambos y transmitir finalmente una contraseña del demandante, que queda protegida. La versión más extendida de este protocolo en entornos de Internet, es aquella en la que el certificado a comprobar es el del servidor, permaneciendo como opcional la necesidad del certificado de cliente. En esquemas que requieren del servicio de *no repudio en origen*, tal certificado se hace imprescindible. A menudo, y para ambos casos, la tarjeta inteligente es el mejor soporte para el material criptográfico y dichos credenciales. Son múltiples los escenarios en los que participa la tarjeta en esta modalidad (p.e. administración electrónica, negocio electrónico, etc.) frente al reto que supone que sea la propia tarjeta la que establezca el túnel de protección, mediante el protocolo TLS por ejemplo, y se comporte como un dispositivo autónomo dentro del sistema de red. Para ello el concepto actual de tarjeta inteligente debe evolucionar, y así está ocurriendo, según otras directrices tecnológicas, tal como veremos a lo largo de esta tesis.

Protocolos basados en técnicas de Conocimiento-Cero (Zero-Knowledge, ZK). Un importante número de esquemas de autenticación están basados en el mismo problema que RSA; es decir, la factorización de un módulo público. En [Fis84] se propuso un esquema donde un número público es el cuadrado módulo un número privado aleatorio. Fiat y Shamir [Fia87] lo mejoraron haciendo que cada número privado fuese el resultado de la firma de Rabin de un elemento de identidad. En [Gol89] también se formalizaron los protocolos de conocimiento cero (Zero Knowledge, ZK); a estos trabajos se sumaron otros que proponían que dichos números privados fueran la raíz cuadrada modulo un número primo pequeño, lo cual implica módulo para cada solicitante de autenticación [Mic90]. Esta técnica se complementaría también con los trabajos en protocolos de conocimiento cero de Guillou y Quisquater [Gui89][Gui90], que proponían inicialmente un protocolo conocido como GQ1, en el que el número privado es una raíz n-ésima modular de un número público, es decir, la firma RSA de un elemento de identidad. (conocimiento cero de una prueba de conocimiento de una firma RSA). A medida que los protocolos fueron mejorando su aplicación a las tarjetas inteligentes no se quedaba atrás; ya en [Bet88] se hizo una de las primeras propuestas.

Posteriormente, de nuevo Guillou y Quisquater, evolucionaron el protocolo GQ1 hacia el que fue llamado GQ2, y consiguieron interesantes resultados en cuanto a eficiencia. En una comparativa realizada por estos autores, con el objetivo de aplicar esos métodos de conocimiento cero en procedimientos de autenticación con tarjetas inteligentes bancarias, concluyeron que el método GQ2 proporcionaba un importante ahorro en coste computacional, lo que permitiría a la tarjeta, incluso, implementar dicho protocolo sin necesidad de criptoprocesador. Como consecuencia, los autores proponían a principio de la década actual la coexistencia de RSA y GQ2, en el aprovecho de las ventajas de ambas técnicas, y la incorporación de ésta última junto a la firma RSA, en los procesos de *autenticación dinámica de datos* de las especificaciones de EMV'96. La técnica original de *autenticación dinámica de datos* en tarjetas inteligentes, fundamentada en conocimiento cero, fue descrita en [Lea95] e incorporada en dichas especificaciones.

Protocolos basados en Contraseña bajo esquemas de Reto-Respuesta. Quizás una de las primeras propuestas de autenticación basada en contraseña haciendo uso de funciones one-way fue publicada por [Lam81] que junto con el trabajo de [Sha84] se establecieron las bases de numerosos trabajos posteriores en esa línea y en los que las tarjetas inteligentes participarían con un papel relevante. Probablemente, la base de la factibilidad e importancia de dichos protocolos de autenticación en estos dispositivos fue llevado a cabo por el trabajo de los reconocidos Abadi y Burrows [Aba93] en donde junto con mecanismos de delegación, basados en el uso de agentes de confianza, se explotaba el potencial de éstos en esquemas basados en contraseñas. El lenguaje formal de explicitar la autenticación descansaba en la lógica desarrollada por Burrows en [Bur90].

A partir de entonces, han sido especialmente prolíferos los trabajos de investigadores de la que podría ser denominada la *escuela asiática* (países como Taiwan, China, India, Malasia, etc.) en esta línea de trabajo. En general, los criterios que deberían servir para realizar la evaluación y comparación de estos protocolos, y en los que se han fundamentado la mayoría de estos trabajos podrían resumirse en:

- La no necesidad de tablas de almacenamiento de contraseñas.
- Evitar la utilización de técnicas de sincronización de reloj.
- Autenticación mutua.
- Computación acorde con la tarjeta inteligente.
- Resistencia a un espectro lo más amplio posible de ataques.

Aún cuando queda clara la importancia de autenticación mutua en esquemas de este tipo y otros, no siempre han sido incorporados como criterio inicial de diseño para tarjetas inteligentes. Así, en trabajos como [Hwa00] y [Lee02] se proponían soluciones interesantes pero que no contemplaban la condición de mutua autenticación. De hecho, hasta 2002 con el trabajo [Chi02] no se proponían por primera vez una autenticación mutua remota basada en contraseña con tarjetas inteligentes. Sin embargo, en el análisis de este esquema fueron encontradas las siguientes desventajas: estar basado en *time-stamps* (que por otra parte requeriría una ajustada sincronización de reloj), además de ser vulnerable a un ataque *off-line* de diccionario con tarjeta, a ataques de sesión paralela [Hsu04], de reflexión [Mit89] y a ataques desde dentro o *insider attack* [KuC04].

De otro lado en [She03] se propuso un esquema algo más pesado pero como también ocurría en el esquema descrito en [Chi02] presentaba ciertas desventajas al estar también basado en *time-stamps*. Junto a éstos, han sido otros los intentos que han insistido en el empleo de estas técnicas en la autenticación mutua con tarjetas inteligentes [Lee04] [Yoo05] [Lia06] .

Más recientemente en el trabajo [Shie06] fue propuesto un nuevo esquema ligero de autenticación mutua basado en contraseña con tarjetas inteligentes. Incorpora todas las ventajas propuestas inicialmente en [Chi02] y [She03] pero poco atinadamente vuelve a hacer uso de técnicas de *time-stamps*, que como se ha explicado anteriormente, queda desaconsejado en todo punto, desde la perspectiva de la atomicidad en el diseño de los protocolos de autenticación, y por ende de la seguridad. En este sentido y por contra, se hace especialmente recomendable, en el diseño de este tipo de protocolos con tarjetas inteligentes, la utilización de técnicas basadas en números de un sólo uso desechables, *nonces,* introducidos ya por Needham y Schroeder [Nee78] .

En [Jua04], cuyo autor había publicado previamente un esquema de autenticación mutua en entornos inalámbricos [Jua99], se adapta dicha solución para la autenticación mutua remota basada en contraseñas con tarjetas inteligentes. Destacamos como una propiedad interesante de este esquema que está basado en *nonces*, evitando así los problemas señalados anteriormente. Otra característica que lo distingue de otros muchos esquemas es que permite acuerdo de clave de sesión. Sin embargo recientemente, en [Pha06] y [Shie06] se señalaron algunas deficiencias en el esquema de Juang. Así, se detectó que en dicho esquema ataques de clave relacionada (*key-related*); además, no se chequeaba la integridad de los mensajes transmitidos y que, en salvaguarda del coste de computación en la tarjeta inteligente, estos mensajes tampoco eran firmados.

En [Fan05], fue presentado un candidato interesante como esquema de autenticación remota mutua para tarjetas inteligentes, basado en contraseñas y haciendo uso de *nonces*. Presenta resistencia al ataque de replicación y a los ataques de diccionario con o sin tarjeta. Al mismo tiempo permite la revocación de tarjetas perdidas sin la necesidad de cambiar la identidad de los usuarios. Este protocolo no contempla la posibilidad de acordar la clave de sesión. Aunque éste introduce características interesantes, desafortunadamente después de analizarlo por este autor [Tor06b] presenta algunas debilidades.

Como conclusión a este apartado, puede apuntarse que han sido muchas las propuestas para la autenticación basada en contraseñas para tarjetas inteligentes, aunque quizás los criterios de partida no siempre han sido muy acertados; en parte, porque no se han considerado las características más realistas de las tarjetas inteligentes más actuales. Por tanto, se hace necesario poder establecer unos criterios más robustos en el diseño de protocolos de autenticación basados en contraseña con tarjetas inteligentes, que permitan concebir soluciones más estables, resistentes a ataques y duraderas, acordes con el potencial de elemento de seguridad que corresponde a éstas. A continuación, se postulan algunos criterios que en nuestra opinión deberían regir tales diseños.

- Tarjeta Inteligente autónoma en el procedimiento de autenticación (self-authenticable); se considera la tarjeta un elemento autónomo e independiente del resto del sistema, por tanto debe incorporar sus propios mecanismos de seguridad y de forma ajena al lector u otras entidades. La

cooperación con otras entidades para la implementación de esquemas de autenticación podrían comprometer las seguridad del sistema.

- Protocolos basados en *nonces*; se desestima cualquier utilización de *time-stamps* dada la incapacidad de la tarjeta inteligente de crearlos por sí misma y evitar ser provista de dichos *time-stamps* por el terminal lector que podría ser un dispositivo malicioso. La generación de *nonces* será autónoma en la tarjeta por sus propios medios y sin la intervención de otras entidades.

- Autenticación mutua; una sólida autenticación mutua debería poder llevarse a cabo independientemente de la existencia de un acuerdo de clave de sesión. El objetivo de la autenticación debería poder conseguirse por cualquier proceso de 3 o 4 cuatro pasos (por ejemplo técnicas de reto-respuesta) independientemente de tal acuerdo, por tanto siendo éste opcional, dependiendo del servicio/ sistema que se trate, puesto que no es mecanismo inherente al proceso de autenticación y está enfocado al cifrado de las comunicaciones posteriores que podría no ser necesario (e.g. control de acceso) y que consumiría recursos en la tarjeta, que no siempre estarían justificados

Kerberos [Neu94] es otro de los protocolos de autenticación basados en contraseña y que responden al esquema reto-respuesta. En este protocolo desarrollado por el MIT, los usuarios disponen de una contraseña secreta conocida por un Centro de Distribución de Claves (KDC). Un usuario A, que desea comunicar con otro usuario B, se autentica contra el KDC, que le facilita un ticket para autenticarse con éste último. Los tickets de Kerberos son considerados como credenciales electrónicos que de alguna manera asocian a su portador ciertos atributos o privilegios. Es conocida de este protocolo la vulnerabilidad a ataques de diccionario off-line, si un atacante logra capturar el intercambio inicial de mensajes entre el usuario A y el KDC. En [Kra92] y [Ito99] se llevó a cabo con éxito la integración de Kerberos v5 en entornos con tarjetas inteligentes; dicho esquema permitía también la autenticación basada en contraseñas y puede considerarse como un ejemplo más de su utilización con este tipo de dispositivos y el potencial que disponían los mismos.

En relación a los protocolos basados en contraseña bajo esquemas de reto-respuesta, es necesario hacer referencia a aquellos que emplean contraseñas de un sólo uso (*one-time password, OTP*). En 1994, Haller publicó un sistema de contraseñas desechables, diseñado para contrarrestar los ataques de reproducción, caso de que la captura de un identificador de registro y una contraseña fuera aprovechada maliciosamente. Dicho trabajo sería publicado como documento de la IETF bajo la etiqueta de *"Informational"* [Hal95]. Este sistema de autenticación hace uso de una frase de paso secreta, a partir de la cual se genera una contraseña de un solo uso. Esta generación se realiza iterativamente a partir de una función resumen o hash aplicada sobre una semilla pública y un secreto (frase de paso).

$$P[0]=H(Semilla, Secreto)$$
$$P[i]= H(P[i-1])$$

Por tanto su resistencia está basada en la irreversibilidad del algoritmo de función resumen empleado. Las contraseñas generadas son utilizadas en sentido inverso, lo que permite al servidor almacenar simplemente la última que ha recibido *P[i]*, y eliminando la anterior; así el cliente se autenticará en un próxima sesión con *P[i-1]*. Con este sistema, sólo dicha contraseña viaja por la red mientras que la frase de paso secreta del usuario nunca lo hace. Como elemento adicional de seguridad, este sistema prevé que ninguna información secreta sea almacenada en ninguno de los sistemas, incluido el servidor a ser protegido. Lógicamente, se trata de un esquema de protección frente a ataques pasivos sobre el sistema de autenticación y por tanto no proporciona protección basados en el aprovechamiento del rastreo de la red, ataques activos u otros de enclavados en técnicas de ingeniería social.

El interés suscitado y la robustez relativa de este sistema, en su campo de aplicación, propiciaron la generalización de este sistema para pasar a denominarse si*mplemente "A One-Time Password System"* y evolucionar hasta la categoría de estándar [Hal98], convirtiendo le S/Key en una herramienta particularizada de este sistema.

Por la propia naturaleza y capacidades de las tarjetas inteligentes, cabía esperar que estos dispositivos fueran propicios para soportar la implementación y uso de sistemas de autenticación basados en OTP, tal como se demuestra en los recientes trabajos [Bic03] [Cha04] [Yoo06].

Probablemente una de las implementaciones comerciales más extendida y que hace uso de técnicas OTP es SecurID [Nys00] ; un *token hardware* desplegado en el mercado por la prestigiosa RSA Security Inc. y que es una implementación concreta del mecanismo de autenticación SASL [Mel06]. Este sistema en lugar de hacer uso de una lista fija de claves, basa su funcionamiento en el empleo de claves dependientes del tiempo. En este caso, el usuario dispone de una token que dispone de una pantalla de visualización (tipo LCD por ejemplo) en donde puede ver un número pseudo-aleatorio, que cambia cada cierto tiempo (entre 30 segundos y 2 minutos) y que queda sincronizado con el servidor de autenticación. De esta manera el usuario, introduce su PIN y el número aleatorio que puede ver, en cada proceso de autenticación a realizar. El servidor verifica que tal información es válida y lo es sólo para ese instante de tiempo. La posibilidad de integrar pantallas de visualización (LCD) y teclados en el formato ISO 7816 hoy por hoy no puede ser considerado como una realidad fuera de los laboratorios; sin embargo, la compañía RSA comercializa dispositivos con otros formatos cuya forma externa se adecua para portar tal LCD, e incluso teclado, al tiempo que gana en usabilidad. Por otro lado, el sistema SecurID no ha permanecido ajeno al interés de los criptoanalistas y se han identificado algunas debilidades. Así, en [Bir04] se delataba la posibilidad de ataques basados la colisión de funciones resúmenes y basándose en la misma técnica en [Con03] el tiempo de ataque podía reducirse incluso, si el atacante dispusiera de cierta información adicional (conocimiento de mayor número de colisiones).

2.2.3. Evolución hacia la Nueva Generación de Tarjetas Inteligentes

Tras este estado de la cuestión referido a la seguridad en las tarjetas inteligentes *convencionales*, en el presente apartado nuestro trabajo se detiene en el estudio de la evolución de estos dispositivos hacia esa nueva generación, que contempla su conectividad a la red mediante la implementación de protocolos de capa 3 y superiores, según OSI. Otros aspectos recogidos en la concepción de la NGTI no se contemplan en el alcance de esta tesis.

Como se ha visto en el presente documento, era predecible que las tarjetas inteligentes adoptaran un papel relevante más allá del de almacén de credenciales o elementos de identificación y aspiraran a participar más *activamente* en entornos de red, y especialmente dadas sus capacidades, en protocolos de seguridad. Así, se vienen realizando recientemente múltiples esfuerzos de investigación orientados hacia el objetivo de convertir la tarjeta inteligente en un dispositivo abierto a la interconexión de redes y considerarlo como un nodo de Internet con la máxima funcionalidad en este sentido, de acuerdo, en la medida de lo posible, a los estándares [Bra89].

En esta línea se han realizado trabajos, como el recogido en [Ree00], que han ido orientados hacia el propósito de establecer una pila de protocolo TCP/IP simplificada de modo que pudiera ser soportada en una tarjeta inteligente y convertirla por primera vez en la historia de las mismas en pequeños servidores web.

La tecnología de las módulos de seguridad (U)SIM no permaneció ausente a todos estos avances, estimulando así nuevas perspectivas en los modelos de negocios, que han favorecido la creación reciente de herramientas genéricas, como SIM Toolkit [SAT06], basadas en tarjetas inteligentes. En este encuadre, estos dispositivos están dotados de cierta pro-actividad y de una conectividad mejorada, a través de un modelo cliente-servidor, en una arquitectura over-the-air (OTA). Esta tecnología está basada en el servicio de mensajes cortos, SMS, y dispone de la posibilidad de actualizar los datos de la tarjeta SIM , así como descargar y activar nuevos servicios, gracias a las aplicaciones OTA. Haciendo uso de esta tecnología se desarrolló un interesante trabajo [Gut00], que conseguía convertir una tarjeta SIM en un servidor web. Si bien es cierto que su implementación no corresponde plenamente a lo establecido en el estándar del protocolo HTTP, el resultado es funcional y efectivo para según que aplicación.

En [Ito00] se extiende por primera vez la infraestructura de Internet para tarjetas inteligentes y define un *middleware* específico con el objeto de proteger las comunicaciones de una aplicación y una tarjeta inteligente a través de la red.

En [Uri00], sin embargo se apostaba por un protocolo del tipo TCP que, sin llegar a cumplimentar todos los requisitos exigidos en dicho protocolo, abordaba el concepto de *internet card* basado en agentes. Desde otro enfoque, en [Don01] [Cha01] [Cha02] se apuntaba de nuevo hacia la implementación de una funcionalidad de tipo proxy, pero que permitía integrar de forma eficiente a las tarjetas en entornos distribuidos y en los que la consolidación de la programación orientada a objetos de JavaCard [Che00] favorecía este proceso como en [ChC01], donde se hacía uso de tecnología Java Card Web Servlet para convertir la tarjeta inteligente en un repositorio móvil de objetos web, que incluiría páginas HTML con datos referentes a la aplicación específica.

Paralelamente, el proceso de evolución de la tecnología de tarjetas inteligentes se vería completado por los avances y desafíos en los sistemas operativos, y que fueron identificados en [Gri03][Dev03].

Sin embargo, las tarjetas inteligentes, como mero elemento con capacidad de almacenar y transportar información particular al usuario de forma segura, también han seguido siendo integradas en el entorno web, tomando ventajas de sus particularidades, al punto de que ciertas propuestas recientes han incorporado las tarjetas en la gestión de las *cookies* de sesión web de usuarios [Cha05].

Como se ha referenciado, en [RES03] un importante número de expertos discutieron sobre los características, pasos y planificación de lo que debería ser una *nueva generación de tarjetas inteligentes* con o sin contactos; quedaba patente la clara evolución hacia una tarjeta inteligente conectada a la red. Trabajos concretos muy recientes, dan forma y especifican cómo serán dichas tarjetas y qué ventajas de seguridad introducen. A continuación se detalla la contribución esencial de dichos trabajos este área, que podrían etiquetarse bajo el concepto en inglés cada vez más utilizado: *network smart cards*.

En [Mon04] y [LuK04a], la tarjeta era ya claramente tratada como un nodo de Internet, que implementaba protocolos de comunicación y de seguridad estandarizados, para conectar con la red vía un host. La tarjeta podía proveer servicios o acceso a recursos en Internet haciendo uso de una pila de protocolos tal como lo haría cualquier otro nodo en la red. Su empleo en esquemas de seguridad no tardaría en proponerse. Así, la tarjeta inteligente en red podría establecer comunicaciones seguras directas con servidores remotos en Internet, tal como se demuestra en [LuK04b]. Esta capacidad permite a las tarjetas asegurar las transacciones *online*. Una comparación con respecto a procesos de autenticación -basados en dos factores- tales como los dispositivos OTP o respecto a las tarjetas convencionales puede encontrarse en [Ali05]. Otros trabajos incidían en la seguridad a más bajo nivel y trataban el filtrado de paquetes por parte de la tarjeta inteligente en diferentes etapas, que irían desde las rutinas del servicio de interrupciones hasta el filtrado propio de la pila de protocolos [LuK06].

Si observamos una tarjeta inteligente tradicional, ésta comunica con un host haciendo uso del estándar ISO 7816. Para ello, dicho host implementa un *middleware* específico instalado con el objeto de comunicar con aquella, y así poder proveer determinados servicios, por ejemplo, de seguridad. Sin embargo, en la tarjeta inteligente en red ningún *middleware* es requerido en el host o en la máquina remota con el fin de hablar con ésta. Para superar este hecho, las tarjetas inteligentes han debido enfrentarse a numerosos desafíos de ingeniería principalmente debidos a sus limitaciones de recursos de computación. Reclamamos atención en este punto, al hecho de que los recursos de la tarjeta están bastante limitados considerando que ésta debería trabajar con tráfico de red en tiempo real. Más allá, la demanda de computación y la comunicación para la tarjeta son incluso mayores cuando se trata de asegurar las comunicaciones, lo que implica la cuota correspondiente de computación criptográfica. En 2003, la primera *network smart card* presentada por Axalto (hoy día Gemalto[5]) disponía solo de 6Kb de RAM y el ancho de banda estaba limitado al interface ISO 7816-3 (half-duplex) para el que se

[5] Desde 2 de Junio de 2006 las compañías fabricantes de tecnología relativa a tarjetas inteligentes Axalto y Gemplus fusionaron sus esfuerzos en una empresa común denominada Gemalto.

requería un protocolo puente denominado *Peer I/O* (se sitúa sobre la capa ISO 7816 y debajo de la capa de red) que permitía su conversión a *full-duplex*. Del mismo modo, en lado del *host* debía implementarse un dispositivo controlador serie (*driver*) con funcionalidades *Peer I/O* que tratara ésta como una comunicación serie común y, por tanto, tampoco se hacía necesario la inclusión de *middleware* adicional.

En los mencionados trabajos [Mon04] y [LuK04a], ya se apuntaba a un interfaz de comunicaciones basado en el estándar USB [USB00]. El empleo inicial de la tecnología USB en tarjetas inteligentes pasaba por una técnica de encapsulación de los paquetes ISO 7816 en paquetes USB. Esta técnica se estandariza en [ISO7816-12]. Una concepción posterior de esta tecnología permite de hablar de una implementación *pura* de USB en las tarjetas inteligentes venideras, con plenas funcionalidades entre las que se incluiría la comunicación serie *full-duplex*. De esta manera, la tarjeta inteligente conecta a Internet a través de un host haciendo uso de la comunicación en serie según el nuevo modelo de USB en redes, *USB Networking Model*, [USB05]. En tal caso, la tarjeta es reconocida por el sistema operativo del *host* como cualquier otro dispositivo conectado a un puerto USB.

En la Figura 2.10 se ilustra un ejemplo de una pila de protocolos para una tarjeta en red con tecnología USB. La conexión hardware entre la tarjeta y el *host* se lleva a cabo mediante ésta. Sobre el controlador USB se implementa un controlador USB EEM (Ethernet Emulation Model), que transporta tramas Ethernet dentro de paquetes USB según [USB05].

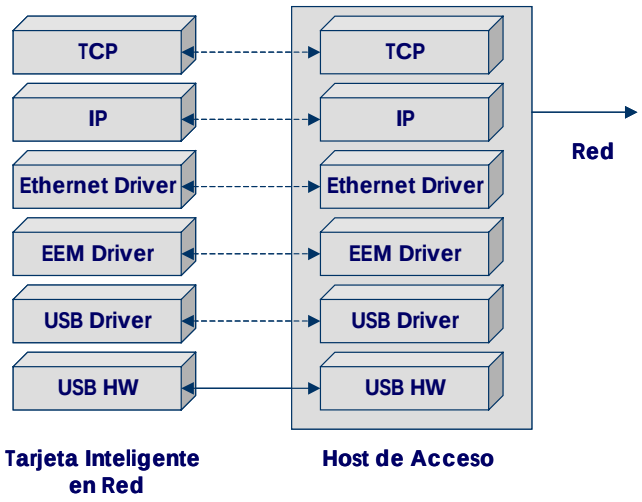

Figura 2.10 Tarjetas Inteligentes en red con interfaz USB según [USB05]

Diferentes compañías fabricantes, como Gemalto, Giesecke & Devrient (G&D), trabajan sobre alguno de estos enfoques de tarjetas inteligentes en red, y reciben nombres como *Internet smart cards* o *web cards*. En concreto, Gemalto trabaja en la actualidad con tarjetas inteligentes sobre la plataforma .NET de Microsoft (Cryptoflex.NET), con comunicación USB, chips de Samsung con microprocesador de 33 Mhz, RAM de 16K, 128K de ROM y 64K de EEPROM. Por su parte, G&D aunque

con prestaciones similares apuesta por tarjetas basadas en Java Card con un mínimo de 24K de RAM.

Con este último enfoque ilustrado en la Figura 2.10, se incide en la posibilidades que ofrece para la comunicación de la tarjeta inteligente con la red sobre los protocolos de capa 2 de la familia IEEE 802, como Ethernet. Este hecho justifica aún más la consideración de redes de acceso basadas en estas tecnologías, tal como se apuntó en la sección 2.1.3.

2.2.4. Avances en la Interconexión de Redes Inalámbricas, PWLAN

Han sido claros los avances en el proceso de estandarización de los sistemas de 4ª generación basados en la interconexión de redes locales inalámbricas y de redes de telefonía de tercera generación [3G-23234][Ahm03]. Basado en el Modelo de Referencia en la interconexión 3G/WLAN para distintos escenarios, descrito en dicho estándar Figura 2.11, se desarrolla de forma paralela un documento de estandarización [3G-33234], y otros trabajos descriptivos [Koi03], relativos a la seguridad involucrada en estos sistemas y que son el objeto principal de estudio en fases anteriores y marco de trabajo para esta tesis. En este contexto, queda patente la proliferación de dispositivos inalámbricos unimodo o multimodo (capaces de establecer conexiones sobre enlaces de distinta naturaleza) y de tamaño reducido, en donde podríamos incluir también las tarjetas inteligentes, capaces de desplegar servicios de seguridad al implementar, entre otros, algoritmos criptográficos de forma eficiente y protocolos seguros.

Si bien es cierto que dicho estándar está descrito para redes locales inalámbricas genéricas, como ha quedado comentado, el objeto de nuestro trabajo se centra exclusivamente en la familia de redes locales inalámbricas de la familia IEEE 802.11. Un arquitectura de interconexión concreta para redes de tecnología de UMTS y del tipo IEEE 802.11 es evaluada y testeada experimentalmente en entornos de simulación en [Sid05].

Conviene reseñar que el modelo representado en la Figura 2.11, está referido al escenario 3 de los seis identificados por 3GPP. El escenario 3 se caracteriza porque además de que el control de acceso y de la suscripción del abonado, está contemplada la posibilidad de que el cliente puede acceder a un conjunto de servicios basados en IP que provee el operador de la red de telefonía móvil, que entre otros podría tratarse de Internet. Aunque esta variante, relativa a la provisión de servicios IP, no recae en el alcance de esta tesis, queda indicado aquí como estimulo para posibles trabajos futuros en esta dirección.

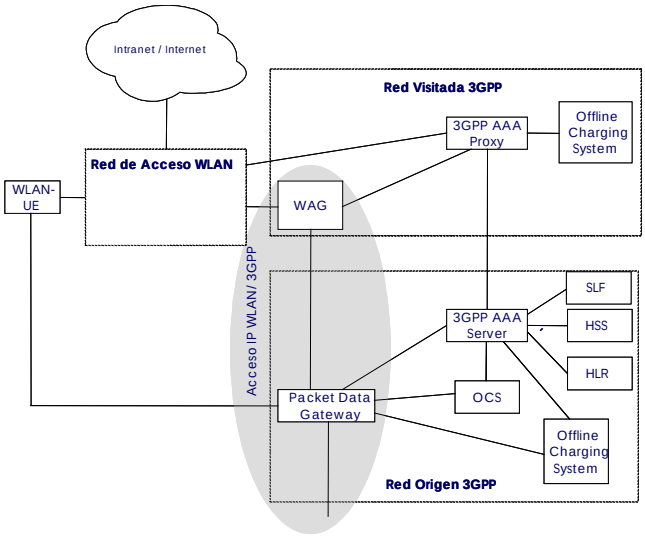

Figura 2.11 Modelo de Referencia para 3G/WLAN según [3G-23234]

En conjunto, estos sistemas quedan por tanto caracterizados por la heterogeneidad de redes de accesos y dispositivos inalámbricos, así como su interoperación. El concepto *all-IP* se hace extensible a la comunicación extremo-a-extremo, mientras un núcleo de red basado en IPv6 completa el esquema, para proveer un variado conjunto de servicios (Web, IMS, VoIP, *Video Streamming*, etc.). Sobre esta materia y desde sus comienzos, han sido múltiples los proyectos europeos que han venido a sumarse [SUI02][BRA01][WIN01][EVO04], desde perspectivas parecidas.

En lo referente a estas redes de cuarta generación, además del soporte que suponen los estándares mencionados, se hace necesaria la referencia de los trabajos de Salkintzis plasmados en las publicaciones [Sal02] [Sal04].

Un enfoque más complejo del modelo referido, incluye la posibilidad de incorporar también la interconexión con proveedores de servicios de Internet inalámbricos, de forma que se pudiera dar soporte a abonados de la red celular de 3G y abonados del W-ISP; en este punto, las técnicas de *roaming* involucradas son merecedoras de estudio [Sur03], para una integración transparente.

Aún no siendo parte del objeto de esta tesis la visión de la arquitectura de interconexión 3G/WLAN desde el plano de las capas superiores en la pila de protocolos, merece destacar algunos trabajos en esta línea, dando cuenta de las posibilidades y avances que esta tecnología demuestra. Así, desde el punto de vista de las aplicaciones prácticas en términos de servicios multimedia sobre IP (IMS) o voz sobre IP (VoIP) prontamente han sido estudiadas y evaluadas sobre este tipo de arquitectura de interconexión con resultados aceptables. Así, el estudio de la calidad de servicio, QoS, no permanecido al margen cuando se ha tratado la factibilidad de proveer servicios ajustados a los requisitos de usuarios. En [Son05], por ejemplo, se llevó cabo un estudio sobre esquemas de control de admisión de llamadas bajo configuraciones de diferenciación de servicios, *DiffServ*. En [Raj05] se evalúa el rendimiento de VoIP bajo un túnel IPsec. En el banco de pruebas se fuerza el número de conexiones sobre un mismo punto de acceso, PA, para valorar la latencia en situaciones de movilidad. También se han

realizado trabajos enfocados a la provisión de IMS en arquitecturas de interconexión como la considerada; en concreto, estudian la interconexión en el nivel de la negociación de sesión, haciendo uso de SIP, protocolo base para proveer IMS [Mar05].

Respecto a los últimos avances de seguridad en 3G/WLAN, conviene resaltar los trabajos de Kambourakis [Kam05] donde se propone una variante para dar soporte de certificados de atributos temporales de los abonados para articular su autorización, minimizando así los inconvenientes relativos a las gestión de los certificados y su revocación. La inclusión de esta infraestructura de PKI se realiza bajo el prisma de reducción del impacto sobre la arquitectura de red existente.

Como se ha mencionado en el epígrafe 2.1.3, los esquemas de autenticación basados en EAP-SIM y EAP-AKA, son las dos propuestas estandarizadas para dotar de este servicio a las arquitecturas de autenticación 3G/WLAN. Son muchas las propuestas aún en borradores de Internet o incluso en publicaciones varias. El empleo de RADIUS o DIAMETER (como servidores AAA) junto con estos marcos de trabajo está cada vez más consolidado y en conjunto pueden considerarse como un enfoque centralizado en el proceso de autenticación. Así, a través de un conjunto de intermediarios (proxys), es posible transportar los mensajes e autenticación de forma segura desde la red visitada hasta una red distanciada del origen. Algunos autores señalan la latencia en la autenticación que esto puede suponer y proponen técnicas basadas en brokers AAA que como tercera parte confiable, TTP, mantiene las correspondientes asociaciones de seguridad y que aspira a ser más eficaz en la distribución de claves [Sal03], mientras que otros trabajos se enfocan hacia un esquema de distribución de claves proactivo, basado en la transferencia de contextos proactivo entre los servidores de autenticación de dos redes distintas (*old* y *new*), sin la necesidad de distinguir entre la red origen o visitante [ShM06] .

En cuanto a los protocolos de autenticación ya referenciados, EAP-SIM y EAP-AKA, recomendados por la 3GPP para la implementación en redes de interconexión 3G/WLAN, algunas deficiencias y vulnerabilidades han sido detectadas:

- ataques que pueden comprometer los vectores de autenticación, especialmente en situaciones de *roaming*.

- en algunos casos, el sistema permite la identificación del usuario mediante la identidad permanente de abonado IMSI en texto en claro, vulnerando la privacidad. Ciertos ataques pueden desplegarse con el objeto de obtener dicho IMSI, intentando suplantar al abonado original.

- la integridad está solo garantizada para los datos de señalización y los datos de aplicación no soportan un *checksum* de integridad asociado.

- no soporta negociación del conjunto de cifrado o negociación de la versión del protocolo.

Ante estos inconvenientes, se ha pretendido dar solución en [Kam04] y, más recientemente en una versión similar, en [Zha06] se aplican esquemas de autenticación basados en EAP-TLS [Abo99] y EAP-TTLS (TLS *tuneleado*) [Fun06] sobre la

arquitectura 3G/WLAN con el objeto de conseguir seguridad extremo a extremo. En este mismo trabajo, se aportan datos sobre una evaluación del consumo y latencia que de ellos se deriva. En EAP Protegido, PEAP, se pretendió superar estas debilidades aplicando TLS y EAP (en un enfoque distinto a EAP-TLS)

2.2.5. Avances en los Protocolos de Autenticación en Capa de Enlace

Como se muestra claramente en el apartado anterior, uno de los marcos de trabajos emergentes es el Protocolo de Autenticación Extensible, *Extensible Authentication Protocol* [Abo04], cuyo objetivo es extender y mejorar el espectro de métodos de autenticación llevados a cabo por protocolos de capa de enlace (capa 2 de OSI); inicialmente descrito para PPP, el protocolo EAP fue más tarde adaptado para proveer servicios a redes de la familia IEEE 802.11 [Sta05].

En [Abo04] puede encontrarse el Modelo de Multiplexación que caracteriza a EAP, Figura 2.12. Este protocolo aísla las tareas de autenticación de las capas inferiores y permite mejorar éstas gracias a otros métodos ya estandarizados, sin necesidad de conectividad IP. De esta manera, EAP puede ser considerado como un protocolo adecuado para autenticar dispositivos en el proceso de registro y acceso a la red. Ha de hacerse notar que EAP no es en sí mismo un protocolo para transportar datos sino una arquitectura para transportar paquetes de otros protocolos de autenticación. Por ejemplo, el protocolo EAP-TLS [Abo99] ofrece un servicio de autenticación basado en el estandarizado TLS, haciendo uso de certificados digitales. La elección de un protocolo de autenticación como EAP-TLS podría darse después de un proceso de negociación entre ambos extremos llevado a cabo mediante el intercambio de mensajes EAP.

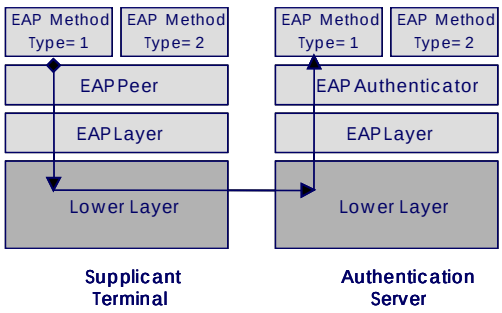

Figura 2.12 Modelo de Multiplexación EAP según RFC 3748

Algunas propuestas más novedosas, como se verá en la próxima sección, apuestan por extrapolar esta visión más allá de las tarjetas USIM/SIM y llevarlas a las tarjetas inteligentes a través de un interfaz definido al efecto.

2.2.6. EAP en Tarjetas Inteligentes

A partir de este enfoque, otros trabajos posteriores [Uri06] [Uri04] se ha apostado por la definición de un interfaz específico para tarjetas inteligentes e implementado en el terminal, que permitiría la selección de un método de autenticación de entre un conjunto disponible y residente en dicha tarjeta. En el Modelo de Multiplexación presentado en la Figura 2.13, se observa como el protocolo EAP se implementa en el terminal y se comunica mediante un intercambio de mensajes a través de un *interfaz de tarjeta inteligente*, con los métodos de autenticación (EAP-TLS, EAP-MD5, etc.).

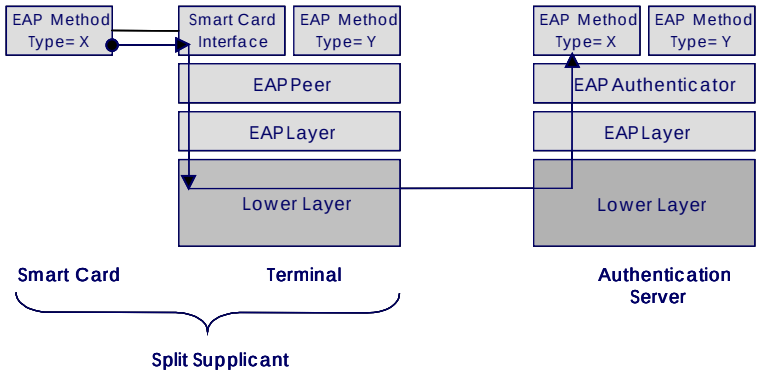

Figura 2.13 Modelo de Multiplexación EAP con Solicitante de Autenticación dividido, según [Uri06]

En principio, desde un punto de vista práctico, el modelo propuesto es resolutivo, sin embargo desde el enfoque de nuestro trabajo quedan pendientes dos aspectos a reconsiderar:

a) se trata de un solicitante de la autenticación dividido (*Split Supplicant*), por tanto ambos dispositivos, tarjeta y terminal, son mutuamente dependientes, y esto se aleja de nuestro propósito, de alcanzar la máxima autonomía posible de la tarjeta como potencial *host* de Internet, es decir, con entidad propia y por tanto auto-autenticable.

b) la seguridad, en general, y el proceso de autenticación, en particular, estaría en gran medida supeditada a este hecho, y podría verse claramente comprometida en el caso de que el terminal, junto con el que participa la tarjeta inteligente, fuese un terminal no confiable; esta última consideración se ajustaría en gran medida a un escenario en entorno público.

Siguiendo un modelo de multiplexación muy similar al expuesto más arriba, el proyecto para *smart cards* de la ETSI [SCP04] considera una variante conceptual del mismo, que queda reflejado en la Figura 2.14.

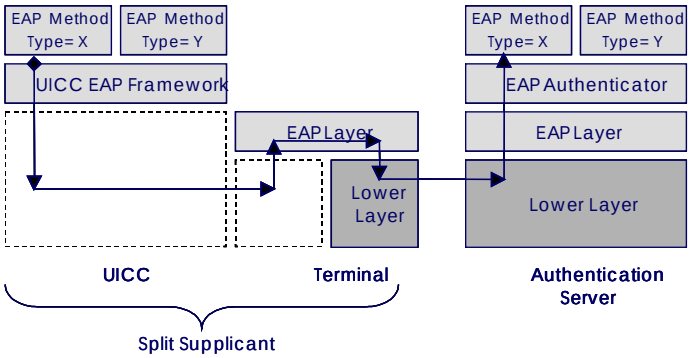

Figura 2.14 Modelo de Multiplexación EAP con Solicitante de Autenticación dividido, según [SCP04]

Aunque con ciertas variaciones (obsérvese que la capa EAP Peer Layer es implementada directamente en la tarjeta bajo la denominación genérica *framework*), la funcionalidad de *Solicitante de Autenticación*, se encuentra de nuevo dividida (*Split Supplicant*) entre el terminal y la tarjeta, presentando con ello los inconvenientes ya indicados en párrafos anteriores. Los protocolos EAP-SIM y EAP-AKA se fundamentan en este modelo de multiplexación.

Capítulo 3.

Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red

3. Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red

En el capítulo anterior, se ha determinado la necesidad de explotar los mecanismos que son provistos en capa 2 para la comunicación de la tarjeta inteligente con la red, que, llegado el caso, le podría permitir el acceso a ciertos servicios. En este capítulo se lleva a cabo, en primer término, el estudio de algunos procesos de autenticación de dispositivos en capa 2, cuyo análisis nos permitirá identificar cuál de estos esquemas se ajusta de mejor manera a los objetivos de esta tesis, así como la posibilidad de aplicación en las tarjetas inteligentes actuales. Posteriormente, se describen un conjunto de propuestas de modelos, requisitos y una arquitectura de protocolos de autenticación para éstas que conforman un nuevo Marco de Autenticación, aplicable a una diversidad de escenarios.

3.1. Estudio y Análisis de Procesos de Autenticación entre Dispositivos

En una primera aproximación, la **autenticación entre dispositivos** podría definirse como los protocolos y mecanismos implementados para tal fin, que de forma automática se ejecutan en ellos sin que el usuario (en caso de existir) intervenga proporcionando dinámicamente *token* lógico alguno (pin, contraseña, frase de paso, etc.), credenciales de seguridad, o activando el envío de mensajes que formen parte del protocolo. No deberían considerarse procesos de autenticación entre dispositivos aquellos que quedan claramente comandados por un entorno de aplicación, a través de APIs de seguridad o criptográficas (*CryptoAPI*), aún cuando éstas sean diseñadas específicamente para la actuación junto con dispositivo o token *hardware* de seguridad (*Cryptoki*, [PKCS#11]). Por tanto, un proceso de autenticación entre dispositivos requiere, en gran medida, la explotación de los recursos de capa 2 y de la autonomía en el proceso de tales entidades, que deberían disponer de sus propios credenciales de seguridad y material criptográfico independientemente de los asociados al usuario o portador de dichos dispositivos.

En algunos casos, bajo esta definición, un proceso de autenticación de usuarios podría consistir total o parcialmente en una autenticación entre dispositivos. Así por ejemplo, en ciertos escenarios de control de acceso lógico o físico, y desde la óptica de un sólo factor de autenticación (algo que se posee), la autenticación de un usuario (por ejemplo, un empleado en el acceso a las dependencias corporativas) podría llevarse a cabo, netamente, mediante la autenticación entre dos dispositivos: tarjeta inteligente y terminal.

El estudio de diversos **casos** representativos, que se describen a continuación, y su posterior análisis nos permitirá identificar posibles formas de enfocar el diseño de los **protocolos de autenticación entre dispositivos en capa 2**. La elección de dichos casos en el presente estudio se ha basado en la representatividad e implantación actual de la tecnologías que incorporan y la estrecha relación que guardan con los intereses de esta tesis. La parte final de este estudio se centrará en analizar qué esquema se ajustaría mejor a las particularidades de la tarjeta inteligente y en qué medida ésta podría implementar las funcionalidades del dispositivo involucrado en el mismo.

Caso 1. Conexión entre dispositivos Bluetooth. Dos dispositivos Bluetooth que tratan de establecer una conexión entre ellos han de proceder con una fase de autenticación durante el establecimiento del enlace lógico mediante el protocolo LMP (*Link Manager Protocol*) [BTv2], tal como se representa en la Figura 3.1. Entre otras funcionalidades, dicho protocolo implementa la autenticación de los dispositivos mediante un esquema de reto-respuesta en el cual el conocimiento del secreto compartido K, por parte de un demandante (*claimant*) es chequeado por un verificador *(verifier*) mediante un protocolo de criptografía simétrica en 2 pasos. El verificador desafía al demandante con un valor aleatorio AU_RAND. Éste devolverá una respuesta SRES como resultado de computar la función de autenticación E_1, que hace uso del secreto compartido K, el valor AU_RAND recibido y su dirección de dispositivo Bluetooth (BD_ADDR) para evitar ataques de reflexión. E_1 implementa el algoritmo de cifrado SAFER+ con una clave K de 128 bits, que podría inicializarse a partir de un valor aleatorio y el octeto formado por el PIN de usuario. La autenticación mutua se llevaría a cabo mediante la ejecución de este protocolo en ambos sentidos.

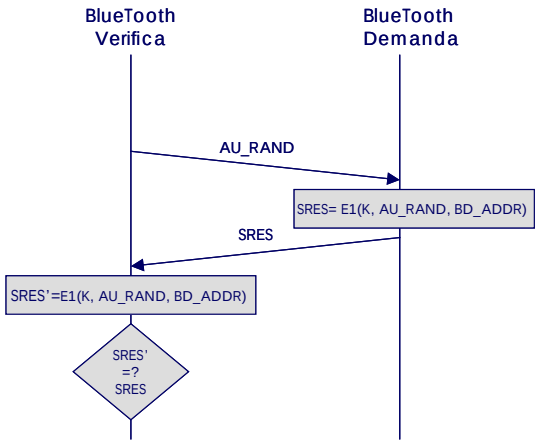

Figura 3.1 Protocolo de Autenticación entre dispositivos Bluetooth

Caso 2. Asociación de un teléfono móvil con una red GPRS. El proceso de autenticación aquí identificado se lleva a cabo, entre otras circunstancias, cuando un teléfono móvil, MS, pretende acceder/asociarse a una red GPRS. Llegado el caso, el nodo de servicio en la red del operador de telefonía móvil SGSN solicita la información de seguridad relativa a un MS determinado (*security related information*) al centro de autenticación HLR/AuC, en el caso de que no disponga de ella en sus registros. Más exactamente, esa información está asociada a un IMSI (*International Mobile Subscriber Identity*) almacenado en el módulo SIM, insertado en ese momento en el MS. A dicha petición, se le dará una respuesta que contiene una lista de pares de valores de RAND(i) y SRES(i). La obtención de estos pares se realiza en el lado de la red, mediante la aplicación del algoritmo A3 a cada valor RAND(i) y haciendo uso de la clave Ki. Estos pares, asociados a cada SIM son almacenados en el SGSN, disponibles para autenticar al abonado cuando proceda, a través de su tarjeta SIM [3G-43020].

Cuando el SGSN lleva a cabo tal autenticación, elige y envía un valor concreto, RAND(j), asociado a dicha tarjeta. Esta transmisión se realiza a través de la red fija y el

enlace inalámbrico, gracias a los servicios de seguridad provistos por el protocolo de gestión de la movilidad y de la seguridad, GMM/SM, sobre la capa 2 de enlace lógico y que se establece entre el SGSN y el MS (ver Figura 2.1). En esencia, dicho protocolo de gestión es el encargado de procurar la autenticación entre los participantes.

El terminal móvil MS transmite esta información a través de la interfaz ISO 7816 mediante un comando tipo AUTHENTICATE a la tarjeta SIM, la cual deberá procesarlo mediante el algoritmo de autenticación A3 y la clave Ki (también conocida por ésta) para calcular el valor SRES(j) correspondiente. La respuesta es enviada a través del mismo protocolo al SGSN, que deberá validar el resultado mediante la comparación con el SRES'(j) calculado previamente. En caso positivo, el usuario a través de su módulo SIM ha sido autenticado y podrá hacer uso de los servicios previstos como abonado de la red (Figura 3.2).

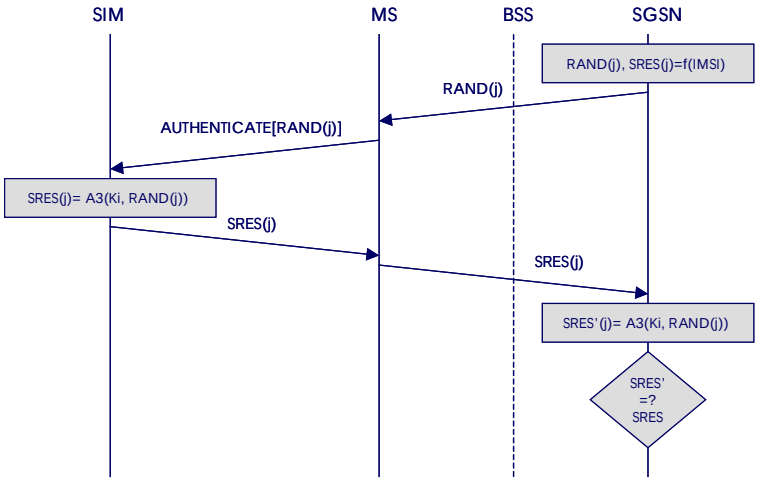

Figura 3.2 Protocolo de Autenticación de MS soportado por la tarjeta SIM

Caso 3. Acceso a una Red Local Inalámbrica IEEE 802.11. El estándar IEEE 802.11[802.11] prevé dos tipos de servicios de autenticación entre dispositivos: abierto (Open System, que en sí mismo no constituye un método de autenticación) y de secreto compartido K (*Shared Key*; la distribución segura de este secreto no se ve contemplada en esta especificación). El tipo invocado en cada momento queda determinado en el contenido de las tramas de autenticación intercambiadas por el protocolo de capa 2, MAC, que controla el acceso al medio. Dichas tramas son enviadas siempre entre un par de dispositivos inalámbricos, por tanto la autenticación *multicast* no está permitida. Esta tecnología garantiza la mutua autenticación entre ambos.

La autenticación de secreto compartido (*Shared Key*) en IEEE 802.11 de 4 pasos es posible tanto si ambas partes o sólo una conocen dicho secreto, K, y sin la necesidad, en este último caso, de enviarlo en claro. Esto es posible mediante la implementación de los mecanismos que incorpora WEP [802.11]. Aún siendo ampliamente conocidas las debilidades detectadas de este protocolo [Stu04][Man05], no es del interés de nuestro trabajo centrarnos en ellas, sino mostrar la visión más conceptual, como esquema de autenticación de dispositivos, que se desprende de esta tecnología inalámbrica.

En un proceso de autenticación de secreto compartido IEEE 802.11 entre un equipo de usuario inalámbrico (WLAN-EU) y un punto de acceso (PA), como el representado en la Figura 3.3, se incluye en el primer mensaje: la dirección (SA) del dispositivo peticionario, el tipo de autenticación a realizar (p.e. AAI = *Shared Key*) y el número de secuencia de la transacción de autenticación (ATSQN). El punto de acceso, PA, da respuesta incluyendo el reto RAND. El valor de RAND, de un total de 128 octetos, se obtiene mediante un texto reto (*challange text*) y se rellena con lo obtenido del generador de números pseudo-aleatorios (PRNG) de WEP. El valor de dicho campo no debe ser estático; por su lado, el valor del par *clave-vector de inicialización IV* es irrelevante para la generación de este reto.

A la recepción de RAND, la estación móvil lo incluye en el tercer mensaje junto con los valores de AAI y ATSQN adecuados y cifra el conjunto con WEP, que hace uso del algoritmo RC4 de *RSA Data Security Inc*. con el secreto compartido K: E_K(AAI, ATSQN, RAND); de esta manera, PA recibe la respuesta SRES que deberá validar, para lo cual primero descifra, extrayendo un valor RAND' que deberá comprobar con el generado por él mismo (RAND). En caso de éxito, PA lo comunicará a WLAN-EU en el cuarto y último mensaje.

El hecho de que el valor RAND y el cifrado del mismo en E_K(AAI, ATSQN, RAND) (mensajes 2 y 3), se incluyan como parte del esquema reto-respuesta, facilitaría la revelación del número pseudo-aleatorio (PRN) para el par *clave-vector de inicialización IV* usado en el intercambio. Así, una implementación correcta exige evitar el uso del mismo par *clave-vector de inicialización IV*, para subsecuentes tramas.

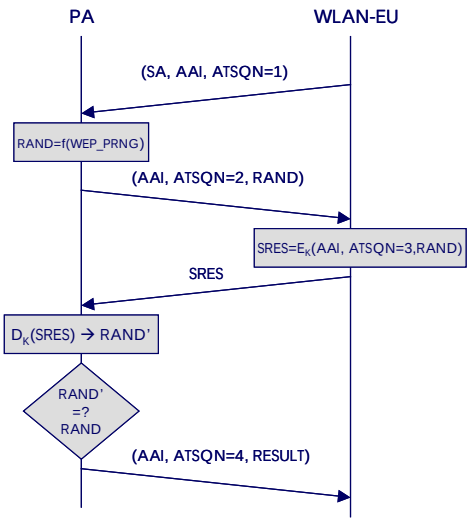

Figura 3.3 Protocolo de Autenticación para el acceso de dispositivo inalámbrico WLAN-EU a una red IEEE 802.11

Caso 4. Acceso a una Red Local IEEE 802 con IEEE 802.1X. La incorporación de la estándar IEEE 802.1X [802.1X] supuso una mejora sustancial en lo que a la autenticación de dispositivos en redes locales IEEE 802 (cableadas e inalámbricas) se refiere. Aprovechando sus ventajas, fue incorporado también al estándar IEEE 802.11i [802.11i] para cubrir las deficiencias detectadas en su predecesor IEEE 802.11, en cuanto a la seguridad se refiere; además de incidir en la autenticación y en los mecanismos de cifrado, lo hace también en las técnicas de establecimiento y gestión de claves. Así, de la mano de IEEE 802.1X, se abría paso a la implementación del protocolo EAP [Abo04] en las redes locales cableadas e inalámbricas. Gracias a IEEE 802.1X, es posible encapsular mensajes de EAP sobre tramas de una red local, expandiendo así a un amplio abanico, las posibilidades de autenticación entre dispositivos con tarjetas de red basadas en IEEE 802. En la Figura 3.4, se muestra un ejemplo de una arquitectura de protocolos para una red local inalámbrica. La implementación del método genérico de autenticación (EAP-type), que contemplaría credenciales de seguridad y algoritmos criptográficos, podría extenderse a un conjunto de posibilidades. Obsérvese en esta ilustración, la incorporación del protocolo RADIUS/EAP [Abo03] para el transporte de mensajes de autenticación entre el punto de acceso PA y el servidor AAA, sobre una red IP.

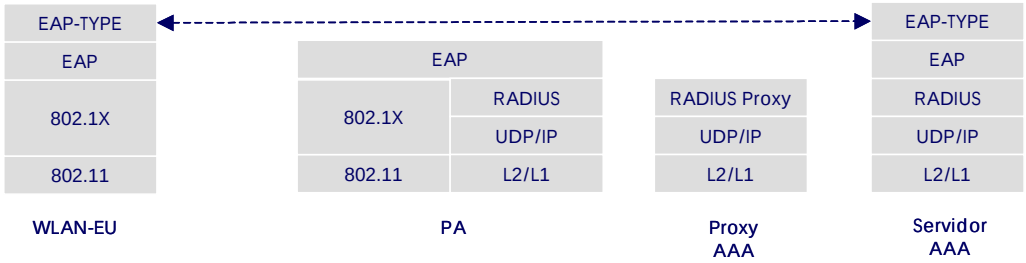

Figura 3.4 Arquitectura de Protocolos para la autenticación con 802.1X/EAP

En este tipo de escenarios de autenticación entre dispositivos, las garantías de seguridad se ven fortalecidas a costa de un conjunto mayor de entidades involucradas y de mensajes de autenticación, debiendo considerar la complejidad que esto introduce en el sistema..

Por simplificar en este estudio, la Figura 3.5 resume la esencia de este tipo de protocolos de autenticación, y del que más tarde podrá encontrarse más detalles en esta tesis

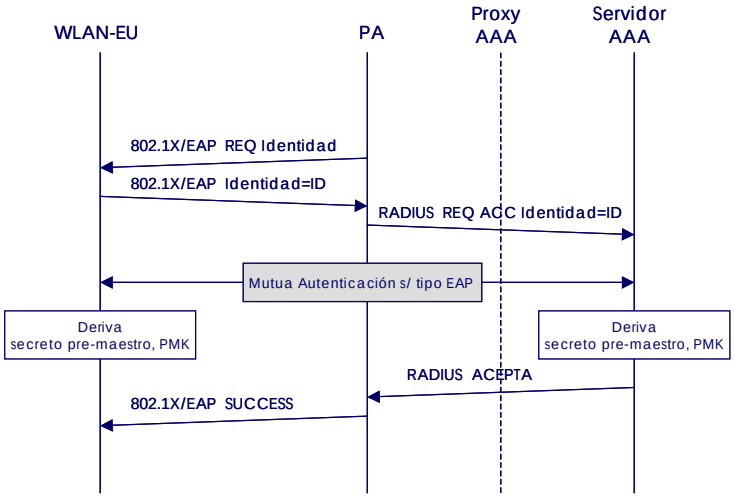

Figura 3.5 Ejemplo Protocolo de Autenticación para el acceso de dispositivo inalámbrico WLAN-EU a una red IEEE 802.11i

3.1.1. Análisis de los casos estudiados

Un análisis detallado de los casos estudiados de autenticación entre dispositivos nos ha permitido identificar un conjunto de características comunes que hace posible la clasificación según dos enfoques distintos y que determinarán la conveniencia de adoptar uno u otro para su aplicación a las tarjetas inteligentes como dispositivos.

Enfoque basado en el Medio de Acceso

En la Figura 3.6a, se representa conceptualmente este tipo de enfoque en el diseño de protocolos de autenticación entre dispositivos. Son representativos de éste, los casos 1 y 3, que se caracterizan por un hecho destacable en primera instancia, al tratarse de esquemas de autenticación *local*. Sin embargo, analizar las consecuencias derivadas y otros factores paralelos, resultan de gran interés.

Autenticación local. En el contexto de este trabajo, una autenticación local entre dispositivos viene determinada por el hecho de que entre el dispositivo demandante (*claimant)* y el dispositivo verificador (*verifier)* no se interponen otras entidades; éstos son los encargados de implementar el protocolo de autenticación y de intercambiar los mensajes oportunos, por sí mismos. Una autenticación local así entendida, prescinde de la necesidad de una infraestructura de red para la fase de autenticación (*autenticación*

off-line), lo cual no implica que no existiera dicha infraestructura para la posterior dotación de servicios una vez superada la misma.

Autenticación distribuida. Como consecuencia de la autenticación local, estos esquemas podrían considerarse autenticaciones distribuidas, en tanto que sería factible integrarlos dentro de esquemas más complejos, basados en la descentralización de los procesos de autenticación y delegando esta funcionalidad a entidades distribuidas en el sistema. Obviamente, además de la pertinente infraestructura de red, técnicas de distribución, gestión de claves y certificados digitales (p.e. para casos de PKI) se harían necesarios.

Autenticación en la asociación/conexión. Los casos 1 y 3 se caracterizan porque se llevan a cabo en los primeros pasos durante el establecimiento de la asociación/conexión entre los dos dispositivos, y por tanto sin la necesidad de que protocolos o aplicaciones de un plano superior intervengan. Podrían considerarse por tanto mecanismos de autenticación *netamente* de capa 2 (*data link layer*). En esta fase, la comunicación entre los dispositivos resulta limitada, y sólo los mecanismos previstos en la capa de enlace lógico permiten llevar a cabo el proceso de autenticación.

Autenticación ligera. Se tratan de mecanismos de mutua autenticación, basados en un sólo factor, y sobre un esquema sencillo de reto-respuesta mediante el intercambio de un conjunto reducido de mensajes de autenticación. La fortaleza de estos procesos residirá en la correcta generación de números aleatorios (retos) y de la implementación del algoritmo criptográfico. Estos aspectos podrían verse mermados en algunos dispositivos de capacidades reducidas, y por tanto suponen un interesante desafío, por ejemplo, para aquellos basados en una interfaz de comunicación RFID.

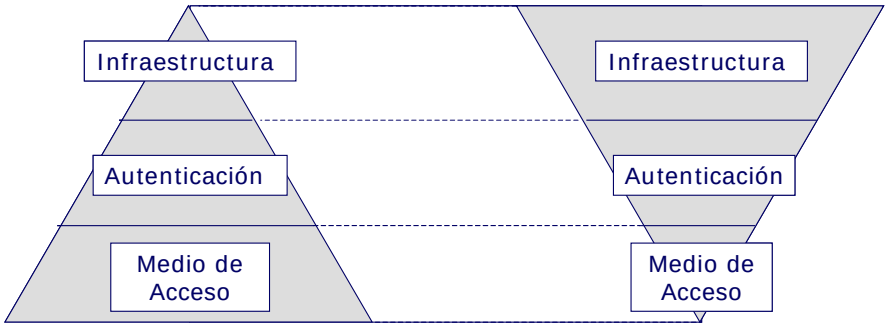

Figura 3.6 Modelado del enfoque en el diseño de protocolos de autenticación de dispositivos

Enfoque basado en la Infraestructura

En la Figura 3.6b, se representa conceptualmente este tipo de enfoque en el diseño de protocolos de autenticación entre dispositivos . Son representativos de éste los casos 2 y

4, en los que, además de la autenticación remota, se deriva un conjunto añadido de características diferenciadoras que conviene destacar.

Autenticación remota (*on-line*). Una autenticación remota entre dispositivos, en el contexto de este trabajo, viene determinada por el hecho de que entre el dispositivo demandante y el dispositivo verificador se interponen otras entidades; ambos son los encargados de implementar total o parcialmente el protocolo de autenticación, que implicaría el intercambio de los mensajes de autenticación oportunos con la colaboración de dichas entidades intermedias. Una autenticación remota así entendida, requiere de una infraestructura de red para la fase de autenticación (*autenticación on-line*). Esta misma infraestructura, sobre la base de los protocolos adecuados permitiría una posible posterior dotación de servicios una vez superada esta fase.

Autenticación centralizada. Disponiendo de una solución de autenticación remota, tal como se ha descrito en los casos 2 y 4, se puede tomar ventaja de la infraestructura de red y el sistema de comunicaciones disponible, para el desarrollo de esquemas centralizados, concentrando el rol de verificador en una única entidad (o un conjunto reducido de ellas). Técnicas de distribución, gestión de claves y certificados (para casos de PKI) también encuentran una posibilidad de aplicación en sistemas así concebidos.

Autenticación con comunicación mejorada. Tal como se infiere de los casos estudiados, los procesos de autenticación se llevan a cabo durante el establecimiento de la asociación/conexión entre los dos dispositivos, pero **además** requieren de protocolos pertenecientes de un plano superior (no necesariamente de capa de red) que colaboran con protocolos de capa de enlace para dotarle de funcionalidades mejoradas. Gracias a ello, la comunicación entre los dispositivos, durante la fase de autenticación se ve enriquecida, resultando esquemas más robustos, escalables e interoperables.

Autenticación robusta. Se trata de mecanismos de mutua autenticación, basados en un sólo factor, y sobre un esquema complejo que prevé el intercambio de un conjunto mayor de mensajes de autenticación. La fortaleza de estos procesos residirá, no sólo en la correcta implementación de los mecanismos y algoritmos previstos, sino además en las garantías del sistema de comunicaciones sobre el transitan los mensajes de autenticación. Tradicionalmente, este tipo de autenticación más pesada ha recaído en dispositivos que presentaban suficientes prestaciones computacionales y adecuados interfaces de comunicación.

Ante el objetivo de considerar la tarjeta inteligente como una entidad o dispositivo autónomo con capacidad de autenticarse y comunicarse , en términos de seguridad, con el sistema, de este análisis se desprenden las siguiente conclusiones:

- el diseño de protocolos de autenticación para tarjetas inteligentes según el enfoque basado en infraestructura, permitiría introducir el concepto *tarjeta inteligente en red* para la dotación de un servicio de autenticación. Al mismo tiempo, esto favorecería el grado de adaptabilidad del diseño del protocolo de autenticación hacia el modo en el que se va a realizar la comunicación, resultando una mejor integración de este dispositivo con el resto del sistema.

- un diseño local (enfoque basado en el medio de acceso), limita en gran medida el potencial de la tarjeta inteligente en movilidad/conectividad al depender en el proceso de autenticación de la adecuación (homologación/certificación en algunos casos) de cada terminal concreto. Un diseño así enfocado no explotaría las ventajas de la integración de la tarjeta inteligente en la red y dificultaría la evolución hacia la nueva generación de estos dispositivos.

- un diseño que tome como referencia el enfoque basado en infraestructura, presenta la ventaja de disponer o extender funcionalidades que se adaptan mejor a los servicios o aplicaciones finales (capas superiores), pudiendo adaptarse a distintas particularidades de éstos, dependiendo de diferentes circunstancias. Por tanto, podría hacer referencia a un diseño de protocolo de autenticación para tarjetas inteligentes más flexible e interoperabe ante los posibles requisitos de usuarios (p.e. preferencias o hábitos en el modo de autenticación) o ante el propio sistema, en aras de proporcionar un servicio continuado y eficiente.

- la necesidad de dicha infraestructura podría constituir en sí mismo una desventaja, salvo, lógicamente, en los casos en que ésta ya estuviera disponible y permitiera la escalabilidad e interoperabilidad. En cualquier caso, en esquemas cuya criticidad no fuese relevante podría considerarse un diseño más ligero basado en el enfoque *local*.

- un enfoque basado en infraestructura nos permitiría la incorporación del terminal en el esquema global de autenticación de forma segura, al estar supeditado al control/interacción de/con otras entidades, además de la propia con la tarjeta, aprovechando ésta, por tanto, recursos que la red ofrece.

La necesidad de soluciones en términos de protocolos de autenticación que permitan llevar a cabo el diseño con un enfoque basado en infraestructura para tarjetas inteligentes, entendiendo ésta como un dispositivo final de la comunicación, con la posibilidad de adoptar los roles de demandante y verificador, nos lleva a la consideración de un esquema fuertemente inspirado en el **caso 4**, puesto que nos permitiría no solo aprovechar las ventajas indicadas en 2.1.3 para la correcta integración (en términos de comunicación) de la tarjeta en la red, sino que al mismo tiempo nos permitiría incorporar una solución en el plano de la autenticación. En los próximos epígrafes se estudian los modelos que son de aplicación en IEEE 802.1X y que nos obligará a analizar el hecho de introducir un dispositivo como la tarjeta inteligente en el esquema global.

3.2. Nuevo Modelo Extendido de Autenticación

Previo a una descripción detallada de los modelos que se tratan en los próximos epígrafes, conviene rescatar la definición de términos que se utilizarán a lo largo de este capítulo. En este caso, la terminología aplicada está basada en la que se indica en [802.1X] por su carácter general y de aplicabilidad extendida a una variedad de contextos, al tiempo que resulta bastante nítida en cuanto a la identificación de los roles de autenticación de cada entidad en todo momento. Así, encontramos:

Solicitante de autenticación (*supplicant*): entidad en el extremo de un segmento punto a punto en una LAN cableada o inalámbrica, que es autenticado por un autenticador en el extremo opuesto del enlace. El término de solicitante de autenticación (*supplicant*) es usado en el mencionado estándar en lugar de otros términos, quizás más convencionales, como *claimant*, *peer o authenticating peer*. En nuestro trabajo, seguiremos este mismo criterio.

Autenticador (*authenticator*): entidad en el extremo de un segmento punto a punto en una LAN cableada o inalámbrica, que facilita la autenticación de una entidad asociada en el otro extremo del enlace. Es, por tanto, la entidad que garantiza y controla el acceso.

Servidor de autenticación (*athentication server*): entidad que proporciona un servicio de autenticación a un autenticador. Este servicio determina, a partir de los credenciales aportados por el solicitante de autenticación (*supplicant*), si éste está o no autorizado para acceder a los servicios que facilita el autenticador. La función del servidor de autenticación puede estar implementada directamente en el autenticador o puede estar en otra entidad (distinta físicamente) a la que se accede a través de una red, a la cual el autenticador tiene acceso. En el contexto de esta tesis, consideraremos la separación física entre ambas entidades, por la completitud y ventajas adicionales que este esquema presenta.

En la Figura 3.7a, se representa el Modelo Genérico de Autenticación que se deriva de IEEE 802.1X y en el que se establecen las relaciones de autenticación entre las entidades que participan en el proceso allí definido, haciendo uso de la nomenclatura que acabamos de definir.

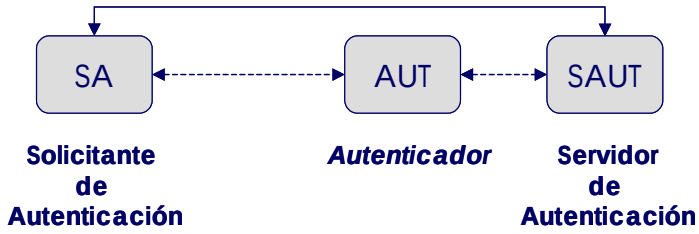

Figura 3.7a Modelo Genérico de Autenticación

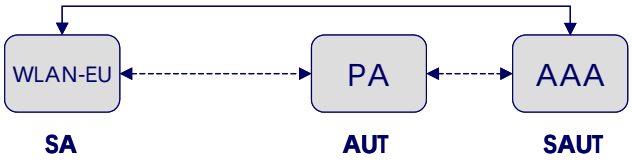

Figura 3.7b Ejemplo de aplicación del Modelo Genérico de Autenticación

en IEEE 802.11i

En la Figura 3.7b, se representa además un ejemplo para dispositivos con tarjetas de red de la familia IEEE 802, y en concreto para terminales inalámbricos acordes con IEEE 802.11i. En general, la entidad EU será el equipo de usuario para el acceso a la red local cableada (LAN-EU) o inalámbrica (WLAN-EU), por lo que podría tratarse de un ordenador PC, una PDA, ordenador portátil, etc. Bajo este esquema, el dispositivo EU adopta el rol de solicitante de autenticación, SA, y establece el oportuno intercambio de mensajes con el *servidor de acceso* o *punto de acceso* a la red, PA, en el rol de autenticador (AUT). Es PA el primer dispositivo con el que entra en contacto mediante un enlace cableado o radio. El *servidor de acceso* o *punto de acceso* facilitará los servicios provistos por el servidor de autenticación, SAUT. Dicho servidor de autenticación dispone del material de clave y la información relativa a los credenciales a validar (además de ofrecer los propios en caso de autenticación mutua) y que adicionalmente podría implementar funcionalidades de autorización y *accounting*, para equipos basados en esquemas AAA. Bajo este modelo, se consigue un esquema de autenticación remota extremo-a-extremo, implementado por las entidades SA y SAUT. Obviamente, por venir *importado* este modelo de la tecnología de red local IEEE 802.1X, se refiere a mecanismos de autenticación implementados exclusivamente en capa 2, según OSI.

Sin embargo, para el objeto de nuestro trabajo, el Modelo Genérico de Autenticación presentado no satisface las necesidades previstas en esta tesis ante la integración de una tarjeta inteligente en el esquema. Según dicho modelo y de forma genérica, la introducción de un nuevo dispositivo, nD, en el lado del usuario y como parte del proceso de autenticación, se vería reflejado, según en el ejemplo anterior, tal como se representa en la Figura 3.8; es decir, nD cooperaría junto con WLAN-EU en las labores de autenticación (*split-supplicant*). Como se ha discutido previamente la situación de *solicitante de autenticación dividido*, se aleja de nuestros objetivos.

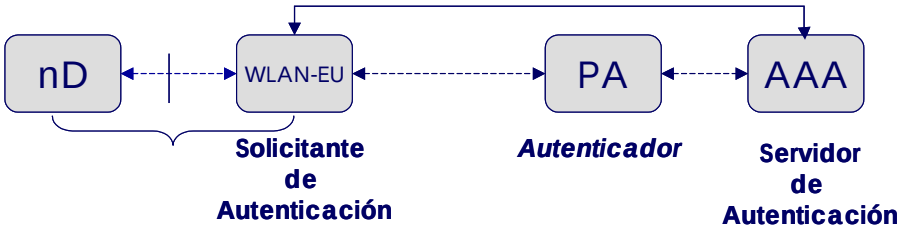

Figura 3.8 Nuevo Dispositivo, nD, en el esquema según el Modelo Genérico de Autenticación

En este sentido, proponemos en esta tesis un nuevo Modelo Extendido de Autenticación, Figura 3.9, que dé cabida a una nueva entidad con funcionalidades de autenticación en el lado del usuario, aunque independiente a éste, y aquí denominado nuevo solicitante de autenticación, nSA.

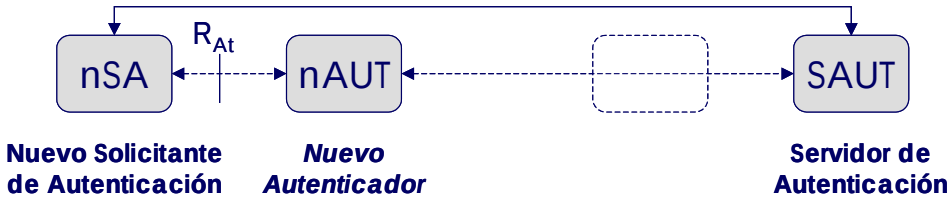

Figura 3.9 Modelo Extendido de Autenticación

Obsérvese en el nuevo modelo de la Figura 3.9, que la entidad introducida nSA establece con SAUT un proceso de autenticación remota extremo-a-extremo, en el que dichas entidades implementan los roles de solicitante y servidor de autenticación, respectivamente. Por su lado, la funcionalidad de autenticador se ve desplazada en el modelo hacia la entidad ya existente que comparte la interfaz R_{At} (*Reference Point, At*) con nSA, apareciendo un nuevo autenticador, nAUT. Esta funcionalidad es adoptada entonces por el EU. Por todo ello, nSA debería disponer de los recursos, elementos y mecanismos de seguridad suficientes como para participar en un proceso de autenticación remota de forma autónoma (credenciales, material criptográfico, computación de algoritmos de seguridad, etc.), independiente de nAUT, y por tanto se requeriría de un diseño atómico de la autenticación, tal como se concibe en esta tesis (ver sección 2.1.1).

La traslación del Modelo Extendido de Autenticación al ejemplo considerado en este epígrafe (Figura 3.7b) se ilustra en la Figura 3.10. El dispositivo solicitante DS (*Supplicant Device*) debería ser distinto del equipo de usuario EU en la red (*LAN* o *WLAN User Equipment*), el cual podría participar a su vez en un proceso de autenticación independiente del llevado a cabo por DS. Conviene recalcar, que el Modelo Extendido aquí definido, ha sido concebido, aunque no es excluyente, para dispositivos DS que no disponen de conectividad de red (p.e. TCP/IP) con el resto del sistema, dadas sus limitaciones iniciales; por tanto, habrá de aprovechar su sistema de comunicaciones en capas inferiores para dotarle de los mecanismos apropiados de autenticación remota en entorno de red. Según el modelo propuesto, el DS establece un enlace físico (con o sin contactos) exclusivamente con el terminal EU a través de la interfaz R_{At}. El dispositivo DS podría intercambiar tramas con dicho equipo de usuario a través de esta interfaz, con el objeto de iniciar la sesión y ganar acceso al resto del sistema, establecer la transmisión/ recepción de mensajes de autenticación y finalizar la sesión. Detalles sobre estos mensajes de bajo nivel en dicha interfaz, quedan al margen del objeto de este epígrafe. De otro lado, según el Modelo Extendido se contempla un proceso de autenticación remota extremo-a-extremo, en el que las entidades DS y AAA implementan los roles de solicitante y servidor de autenticación respectivamente.

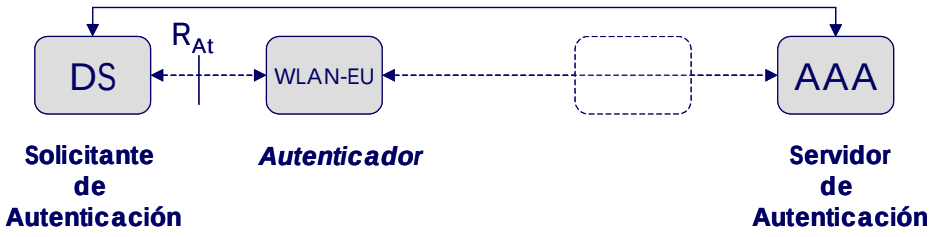

Figura 3.10 Ejemplo de un esquema de autenticación basado en el Modelo Extendido de Autenticación

Por simplicidad, en las Figuras 3.7a y 3.9 que ilustran los modelos, no se ha representado la situación de *roaming*, aunque éstos seguirían siendo válidos y su funcionalidad sería plena. En tal caso, la petición de autenticación sería redirigida desde el servidor SAUT (servidor AAA), que en dichas circunstancias actuaría como servidor de autenticación intermediario (proxy SAUT) en la red visitada, hacia tal servidor SAUT en nuestra red, cuyo operador nos reconoce como registrado o abonado.

En nuestro Modelo Extendido de Autenticación, tal como ocurría con el original, el servidor SAUT con funcionalidad AAA podría establecer múltiples procedimientos de autenticación, entre cuyos solicitantes podrían estar DS y EU. El servidor de autenticación AAA tiene acceso a los registros apropiados para la autenticación y autorización de DS, de donde extraerá la información necesaria para llevar a cabo su tarea en cada caso. Previamente, y de una forma similar, el EU podría ser autenticado en la misma red. En ambos casos, el servidor de autenticación AAA comunicaría la información de autenticación a la propia red local cableada o inalámbrica a los efectos oportunos, con el fin de permitir el acceso a los servicios finales a los que los dispositivos DS o EU pretendieran acceder. Dado que los procesos de autenticación de EU corresponden al modelo *tradicional*, no es del interés de este trabajo entrar en detalle sobre estos procesos, más allá de las necesidades que la autenticación de DS requiera en el modelo extendido, y de la que se dará oportuna cuenta. Por tanto, sobre el Modelo Extendido de Autenticación debe entenderse que junto con la funcionalidad de *autenticador*, el EU debe servir de portador de acceso (conectividad en capa 2) a los servicios de autenticación remotos para el DS, ya que éste por sí mismo no dispone de dicha funcionalidad y es íntimamente dependiente del terminal EU en este sentido. Este último aspecto presenta ciertas implicaciones de seguridad que son analizadas en el próximo apartado.

Es importante resaltar en este punto, que los servicios de interés de estudio, para los que se elabora el Modelo Extendido de Autenticación, y como indica su nombre, son sólo aquellos referidos a los procesos de autenticación en capa 2, excluyendo así todos los

mecanismos y técnicas que tienen que ver con la provisión de servicios, por ejemplo de tipo IP, a los que se accedería según ambos modelos, en los escenarios que tuvieran cabida, una vez superada la fase de autenticación. Siendo así, las entidades involucradas en los procesos de autenticación conforman el núcleo de nuestro estudio, recayendo por tanto las aplicaciones o servicios ulteriores en el objeto de trabajos futuros.

Como se ha mencionado, han sido pocos escenarios en los que DS toma un papel relevante como dispositivo de red autónomo con capacidad de autenticarse ante el sistema en los términos que en esta tesis se entiende, y es precisamente en ese tipo de escenarios en los que nuestro trabajo pretende incidir; se promueve así una solución efectiva para la integración del dispositivo DS como parte del esquema global. Como particularización del problema, podríamos considerar un escenario potencial en el que una tarjeta inteligente (en el rol de DS) podría autenticarse por sí misma ante un servidor de autenticación, AAA. Así, el comportamiento de dicha tarjeta puede ser comparado, por ejemplo, al de un ordenador portátil intentando ganar acceso autenticado a una red local (cableada o inalámbrica). Más allá, el EU, puede ser visto como un punto de acceso PA a tal red que incorpora las funcionalidades de autenticador y de terminal lector de la tarjeta.

Sin embargo, el modelo propuesto sólo identifica los roles y relaciones de autenticación correspondientes a las entidades participantes. Un adecuado análisis de seguridad nos obligará a concretar un conjunto de requisitos, asociados al Modelo Extendido de Autenticación, cuyo cumplimiento se hará indispensable para hacerlo efectivo, desde el punto de vista de las garantías de seguridad en los procesos de autenticación que se basen en él.

3.3. Requisitos de Autenticación

A falta de una arquitectura de protocolos de autenticación concreta, que se elaborará sobre el Modelo Extendido de Autenticación, se realiza un análisis previo que considera los aspectos de seguridad que se derivan de éste.

En tanto que la entidad nSA presenta una alta dependencia de AUT para establecer un procedimiento seguro con el servidor de autenticación SAUT, habrá de prestarse especial atención al uso y protección de la identidad que soporte el primero con objeto de garantizar en la medida de lo posible el anonimato frente al dispositivo de acceso (EU), así como la confidencialidad de los mensajes intercambiados.

El Modelo Extendido de Autenticación ha de partir de la consideración de que las entidades nSA y nAUT sean mutuamente no confiables, para asegurar el establecimiento de medidas de seguridad orientadas a evitar ataques de distinta índole. Así, los posibles ataques de hombre en medio que sobre este modelo darse deberán ser prevenidos sobre técnicas de mutua autenticación, así como, de todos aquellos ataques basados en la modificación de los paquetes bajo distintas técnicas; por tanto, la arquitectura de protocolos de autenticación perseguida deberá proveer mecanismos de protección de la integridad y contra la reproducción de los mensajes de autenticación.

Adicionalmente, deberá garantizarse que la negociación de los métodos, algoritmos o conjuntos de cifrados inherentes a los procesos de autenticación se realice al alza, asegurando que ningún ataque de elementos intermedios fuerce una negociación hacia las soluciones más débiles, dando cabida a las consecuentes vulnerabilidades de seguridad.

Partiendo de estas implicaciones de seguridad, se hace necesario la definición de unos requisitos asociados al Modelo Extendido de Autenticación que aspiran a maximizar la seguridad global del proceso.

3.3.1. Definición de los Requisitos de Autenticación

Para una posterior concepción de una nueva arquitectura de autenticación basada en el Modelo Extendido de Autenticación descrito, se hará necesario el establecimiento de unos requisitos de autenticación, que deberían cumplir las implementaciones basadas en aquel, con el objeto de alcanzar los objetivos que fundamentan nuestro trabajo y evitar o minimizar las debilidades de seguridad de distinta naturaleza identificadas en el apartado anterior. Tales requisitos, que se enuncian a continuación, deberían servir de directrices para la definición de una nueva arquitectura que incorpore la figura de la entidad nSA y soporte los sucesivos pasos a dar a lo largo de esta tesis.

Requisito 1, R1: Autenticación remota entre dispositivos según un enfoque basado en infraestructura, según se define en el contexto de esta tesis. La entidad nSA debe participar autónomamente en el rol de solicitante de autenticación (*Supplicant*) sin la participación activa del terminal (en el rol de AUT) o del usuario; es decir, un solicitante de autenticación no dividido (*non-split Supplicant*) y que por tanto responda a un diseño atómico del protocolo de autenticación. La entidad nSA debe proporcionar sus propios credenciales de seguridad y estos deben ser diferentes de los del usuario y del terminal, con el objeto de alcanzar un nSA auto-autenticable (*self-authenticable*). Los credenciales deben ser inaccesibles mediante cualquier método software o hardware.

Requisito 2, R2: Autenticación mutua extremo-a-extremo ante un servidor de autenticación remoto **mediante protocolos de capa 2** (según OSI) y por tanto previo a una posible conectividad IP (considerada también extremo-a-extremo), sobre una arquitectura potencialmente heterogénea, con nodos de diferente naturaleza que podrían ser origen o puente de ataques, atentando contra la seguridad del conjunto del sistema. Se considerará que se trata de un protocolo de capa 2, cuando al menos para alguno de los extremos de la comunicación dicho protocolo esté implementado en tal capa. Como se ha señalado, la entidad nSA y el servidor de autenticación SAUT deben ser entidades extremo de comunicación en el esquema completo y debe existir un proceso previo de registro *contractual* entre ambos, que queda al margen del alcance del modelo. Al mismo tiempo, los extremos de la comunicación deben ser capaces de implementar funcionalidades tanto de solicitante de autenticación (*supplicant*) como de autenticador (*authenticator*), para permitir una autenticación mutua, y por tanto reforzar la seguridad

del proceso. Ha de observarse que este requisito no exige una simetría en cuanto al método de autenticación; es decir, que ambas partes en una misma sesión recurran al mismo mecanismo o protocolo de autenticación; si bien, la existencia de protocolos simétricos, en el sentido aquí señalado, podrían resultar más eficientes y por ende más robustos. Como un caso particular de autenticación, este requisito *R2* no excluye procedimientos adicionales de autenticación entre otros participantes para escenarios concretos.

Requisito 3, R3: Autenticación en la interfaz AUT-SAUT. La entidad AUT se autenticará previamente por sí misma, sobre el mismo esquema, en el sentido descrito por el Modelo Genérico de Autenticación. Según dicho modelo, debe existir una relación de confianza entre AUT y SAUT basada en técnicas seguras de autenticación mutua de secreto compartido. La distribución de tal secreto deberá de realizarse por un canal seguro distinto a los que proporcionaría el propio esquema de autenticación.

Requisito 4, R4: Negociación segura y flexible del conjunto de mecanismos y de algoritmos de cifrado disponibles, durante el proceso de autenticación. Esto pude ser considerado como un requisito de propósito general en tanto que es definido aquí para cubrir las diferentes implementaciones o versiones de los protocolos y la variedad de características de los participantes en el esquema extremo-a-extremo. Por lo tanto, esto permite ajustar el nivel de seguridad y complejidad del algoritmo a emplear, dependiendo de cada contexto. En casos en los que la criticidad del sistema lo requiera, esta negociación se verá forzada por las directrices y políticas de seguridad de las entidades que intervengan.

Requisito 5, R5: Capacidad escalable de la gestión de las claves. Nuestro enfoque podría tener un efecto relevante en el rendimiento del servidor de autenticación en tanto que debería atender las peticiones proveniente de un importante número entidades nSA en línea.

Requisito 6, R6: Protocolos Estandarizados. El diseño de una arquitectura de protocolos de autenticación sobre el Modelo Extendido de Autenticación estará basado en protocolos y técnicas reconocidas y de solvencia; estandarizados o en proceso de estandarización, no será recomendable la inclusión de nuevos mecanismos o mensajes de autenticación, u operaciones que obligaran de nuevo a un exhaustivo análisis de seguridad del modelo, sino que por el contrario la fortaleza de la arquitectura resida en la demostrada por cada uno de los elementos (protocolos) que la componen. Para ello, la integración de dichos elementos será también respetuosa con los estándares, para preservar en todo momento las garantías de seguridad que de forma inherente aportan.

Así, con una arquitectura basada en Modelo Extendido de Autenticación y en cumplimiento de estos requisitos asociados, se incorporan las directrices para contrarrestar las posibles vulnerabilidades y ataques identificados previamente.

3.4. Análisis de Seguridad basado en las Relaciones de Confianza

Previamente a proceder con el análisis de seguridad basado en las relaciones de confianza, se parte en este epígrafe de la definición de un modelo de confianza y de la terminología necesaria.

3.4.1. Modelo de Confianza Genérico

En nuestro trabajo es necesario determinar un modelo conceptual donde las relaciones de confianza entre las entidades involucradas sean evaluadas cualitativamente. En la Figura 3.11, se ilustra el Modelo de Confianza Genérico que pretende establecer las relaciones de confianza entre las tres entidades que participan en el proceso de autenticación remota, según el Modelo Genérico de Autenticación de la Figura 3.7a. El Modelo de Confianza Genérico aquí presentado se deriva por tanto de [802.1X]. Esta forma de modelar las relaciones de confianza entre las entidades participantes, que ha sido empleada de forma similar y para distintos objetivos en diversos trabajos [Bar04][3G-33234], no pretende ahondar en la complejidad de los estudios teóricos que abordan este tema desde un espectro de perspectivas: confianza centralizada o distribuida [Abd97], modelo basado en las clases directo/recomendación [Abd97], modelos basados en reputación [Xio03], modelos de confianza dinámicos [Liu04] [Xiu05], modelos que incorporan métricas para la evaluación cuantitativa de las relaciones de confianza [Man00], etc. Por contra, el modelo de la Figura 3.11 identifica claramente las posibles relaciones de confianza entre las entidades participantes, asociadas exclusivamente a un proceso de autenticación.

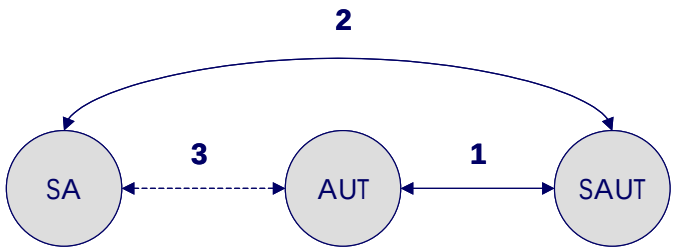

Figura 3.11 Modelo de Confianza Genérico

El valor cualitativo que puede tomar cada uno de los interfaces numerados del 1 a 3 según nuestro modelo se reduce a tres posibilidades: *confianza explícita*, *confianza implícita* o *confianza nula*. Tras un primer análisis y para una correcta comprensión del modelo, se proponen en nuestro trabajo las siguientes definiciones formales de tales términos.

Definición 3.1. Un *esquema de autenticación, E*, es una única solución, que podría establecerse en varias fases, para la autenticación de dos o más entidades, que se ven

relacionadas mediante un modelo de autenticación y, normalmente, en cumplimiento de ciertos requisitos.

Definición 3.2. *Confianza explícita* es el valor cualitativo que toma la relación de confianza entre dos entidades en un esquema de autenticación, *E*, sí y solo sí, se cumple una de las siguientes condiciones:

(a) dichas entidades se han autenticado mutuamente a través de un secreto compartido K, que ha sido previamente establecido de forma totalmente segura, y distribuido mediante un canal seguro independiente del esquema de autenticación *E*.

(b) dichas entidades se han autenticado mutuamente, siendo *E* un esquema de autenticación basado en el Modelo Extendido de Autenticación y en cumplimiento de los Requisitos de Autenticación enunciados.

Nótese que el cumplimiento de (b) exige del cumplimiento de (a).

Definición 3.3. *Confianza implícita* es el valor cualitativo que toma la relación de confianza entre dos entidades A y B en un esquema de autenticación *E*, sí y solo sí, se cumplen las siguientes dos condiciones:

(a) no existe una relación de *confianza explícita* entre A y B en los términos de la *Definición 3.2*.

(b) existe una entidad C, perteneciente al mismo esquema de autenticación *E* , tal que se haya establecido previamente una relación de *confianza explícita* entre B y C y una relación de *confianza explícita* entre A y C, en los términos de la *Definición 3.2*.

Definición 3.4. *Confianza nula* es el valor cualitativo que toma la relación de confianza entre dos entidades en un esquema de autenticación *E*, cuando no existe entre ellas una relación de *confianza explícita* ni de *confianza implícita* en los términos descritos en la *Definición 3.2* y *Definición 3.3*, respectivamente. Cuando en referencia a los modelos de confianza aquí expuestos se califiquen a dos entidades como *no confiables*, deberá entenderse que entre ellas existirá una *confianza nula*, atendiendo a esta definición.

Sean las entidades A, B y C las entidades participantes en un único esquema de autenticación E basado en el Modelo Extendido de Autenticación y en cumplimiento de los Requisitos de Autenticación enunciados. Considérese: α como la expresión de la *confianza explícita*; β como la expresión de la *confianza implícita;* y ϕ como la de la *confianza nula*; todos ellos como valores cualitativos de la relación de confianza entre dos entidades. Sea A $\leftarrow \rightarrow$ B la representación de la relación de confianza entre A y B.

Podemos representar formalmente las relaciones de confianza según las definiciones anteriores de la siguiente manera:

$$E = \{A,B,C\};$$
$$A \leftarrow \phi \rightarrow B;$$
$$if\ (B \leftarrow \alpha \rightarrow C)\ \&\&\ (A \leftarrow \alpha \rightarrow C)$$
$$then\ A \leftarrow \beta \rightarrow B;$$

Obsérvese la aplicación de la propiedad de *transitividad condicional*. Si bien la propiedad de *transitividad* podría expresarse de forma genérica como,

$$A \leftarrow \phi \rightarrow B;$$
$$if\ (B \leftarrow \alpha \rightarrow C)\ \&\&\ (A \leftarrow \alpha \rightarrow C)$$
$$then\ A \leftarrow \alpha \rightarrow B;$$

la *transitividad condicional* exige la introducción de una condición que en nuestro caso viene impuesta por, $E = \{A,B,C\}$ donde E es un esquema de autenticación que, como hemos mencionado, responde a un modelo y requisitos concretos.

Tras estas definiciones y formalizaciones, procedemos con el análisis en detalle de cada interfaz, según la Figura 3.11.

Análisis de las Relaciones de Confianza en el modelo genérico

Interfaz 1. Existe una relación de confianza entre las entidades AUT y servidor SAUT que queda consolidada como *confianza explícita*, en la medida en la que se implementen mecanismos y protocolos robustos de mutua autenticación sobre esta parte de la red, normalmente cableada, basados en secreto compartido y establecido mediante canal independiente y seguro.

$$E = \{SA, AUT, SAUT\};$$
$$SA \leftarrow \phi \rightarrow AUT;$$
$$AUT \leftarrow \alpha \rightarrow SAUT;$$

Interfaz 2. Para la determinación de la relación en esta interfaz como de *confianza explícita*, son requeridos protocolos de autenticación remota extremo-a-extremo en la Interfaz 2 respetuosos con los requisitos de autenticación enunciados y que, por tanto, permitan involucrar a la entidad SA (materializada en el terminal EU) y al servidor SAUT como tales extremos. Para ello, se hace indispensable la colaboración de la

entidad AUT para el transporte de los mensajes de autenticación oportunos, previamente vinculada de forma confiable a SAUT por la Interfaz 1.

$$E = \{SA, AUT, SAUT\};$$
$$SA \leftarrow \phi \rightarrow AUT;$$
$$(SA \leftarrow \alpha \rightarrow SAUT); \qquad \Rightarrow (AUT \leftarrow \alpha \rightarrow SAUT)$$

Interfaz 3. Esta interfaz parte de la consideración de *no confiable* o *confianza nula*. Es sin duda, además, la más sensible a las posibles vulnerabilidades de seguridad (conviene no olvidar que en el contexto de esta tesis podría tratarse también de un enlace radio) y por tanto del valor cualitativo de la confianza aquí será altamente dependiente de otros procesos de autenticación adicionales (interfaces 1 y 2), que de resultar ser explícitos, la Interfaz 3 quedaría caracterizado como de *confianza implícita* (representada con línea discontinua) una vez completado el proceso.

$$E = \{SA, AUT, SAUT\};$$
$$SA \leftarrow \phi \rightarrow AUT;$$
$$(AUT \leftarrow \alpha \rightarrow SAUT);$$

$$if\ (SA \leftarrow \alpha \rightarrow SAUT)$$
$$then\ SA \leftarrow \beta \rightarrow AUT;$$

En este epígrafe hemos analizado la seguridad del esquema basado en el Modelo Genérico de Autenticación a través de las relaciones de confianza entre las entidades que intervienen; sin embargo, este análisis es sólo aplicable a dicho modelo. Procedemos en el siguiente apartado con la definición de un modelo de confianza que se ajuste a nuestro modelo extendido, para a continuación desarrollar el análisis correspondiente.

3.5. Modelo de Confianza Extendido

3.5.1. Descripción del Modelo de Confianza Extendido

Dada la ampliación que proponemos en nuestro trabajo, y que queda reflejada en el Modelo Extendido de Autenticación, se hace necesaria una redefinición del modelo de confianza presentado en la Figura 3.11, en el que, debido a la inclusión de un nuevo elemento solicitante de la autenticación, nSA, extremo-a-extremo, las relaciones de confianza entre todas las entidades participantes deben ser estudiadas nuevamente de forma global. En la Figura 3.12, se representa el Modelo de Confianza Extendido que proponemos en nuestro trabajo, como consecuencia de este hecho.

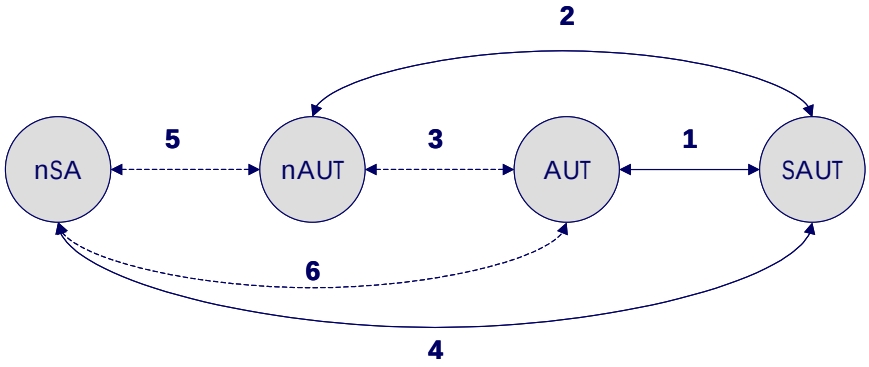

Figura 3.12 Modelo de Confianza Extendido

Análisis de las Relaciones de Confianza en el modelo extendido

En el presente modelo aparecen nuevas relaciones de confianza a ser evaluadas, en las interfaces 4, 5 y 6, y por tanto son objeto de análisis en este epígrafe. Las interfaces de 1 a 3 han sido ya descritas y analizadas en el punto anterior.

La premisa de partida podría fijarse en el hecho de que el anterior dispositivo solicitante de autenticación, SA, que se presenta ahora como nuevo autenticador, nAUT, facilita el acceso de nSA a los servicios de autenticación de la red, y que la relación de confianza que une a ambos puede calificarse a priori de *no confiable o confianza nula*:

$$E = \{nSA, nAUT, AUT, SAUT\}$$
$$nSA \leftarrow \phi \rightarrow nAUT; \qquad \text{(interfaz 5)}$$

Por el análisis descrito en el epígrafe anterior y bajo las condiciones mencionadas, podríamos incluir como premisa que entre nAUT y SAUT existe una confianza explícita,

$$nAUT \leftarrow \alpha \rightarrow SAUT; \qquad (interfaz\ 2)$$

Si se establece un proceso de autenticación mutua mediante un esquema de autentiación E basado en el Modelo Extendido de Autenticación y en cumplimiento de los Requisitos de Autenticación enunciados, tal que $nSA \leftarrow \alpha \rightarrow SAUT$, el análisis respondería a la siguiente lógica:

$$E = \{nSA, nAUT, AUT, SAUT\}$$
$$nSA \leftarrow \phi \rightarrow nAUT;$$

$$if\ (nAUT \leftarrow \alpha \rightarrow SAUT)\ \&\&\ (nSA \leftarrow \alpha \rightarrow SAUT)$$

$$then\ (nSA \leftarrow \beta \rightarrow nAUT); \qquad (interfaz\ 5)$$

En la Figura 3.13, se representa de forma simplificada el Modelo de Confianza Extendido acorde con este resultado, por el cual el valor cualitativo de la relación de confianza en la Interfaz 5 (en línea discontinua) es de *confianza implícita*.

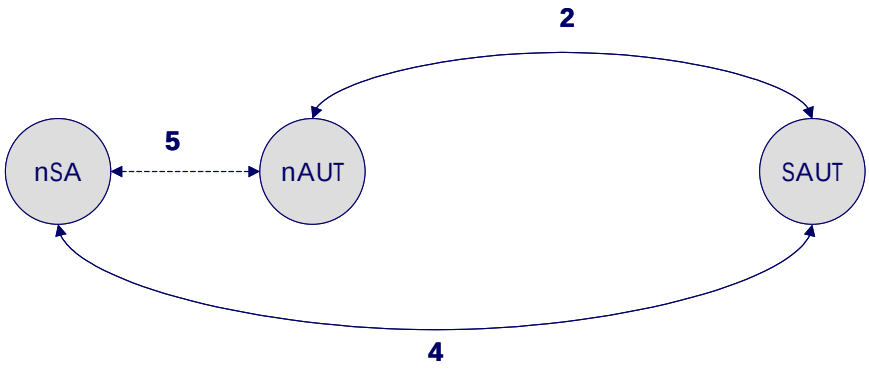

Figura 3.13 Simplificación del Modelo de Autenticación Extendido

A continuación se realiza al análisis de los interfaces, en el que se incluye además la perspectiva de los dispositivos, más allá del rol en el modelo de autenticación.

Interfaz 4. La relación de confianza entre el nSA (DS) y el servidor de autenticación SAUT está caracterizada por el hecho de que, en nuestro caso, el primero está registrado en una entidad o red concreta que provee servicios AAA. Así, deberían implementarse mecanismos de autenticación remota extremo-a-extremo entre ambas entidades que den cumplimiento a los requisitos de autenticación enunciados y que implica el reenvío transparente en los elementos intermedios, como PA (AUT). Siendo así, la Interfaz 4 quedaría calificado como de *confianza explícita*, entendiendo que la autenticación previa entre EU (nAUT) y AAA ha resultado exitosa; es decir, la Interfaz 2 también representa una *confianza explícita.*

Interfaz 5. El terminal EU (nAUT) debe ser considerado a priori como *no confiable* por DS (nSA), especialmente cuando fueran dispositivos pertenecientes a distintos dominios y no cupiera la posibilidad de una autenticación local. No hay que olvidar que este terminal podría estar en cualquier ubicación física y que podría haber sido manipulado para llevar a cabo distintos tipos de ataques contra el dispositivo portátil solicitante de la autenticación, DS. Dando respuesta al modelo extendido y a los requisitos de autenticación propuestos, la Interfaz 4 habría resultado de *confianza explícita* y por tanto la Interfaz 5, que relaciona DS y EU, se podría calificar de *confianza implícita*, Figura 3.13.

Pero más allá, siguiendo el mismo análisis podríamos concluir afirmando que el valor cualitativo de la relación de confianza entre nSA y AUT (PA) es de *confianza implícita* ($nSA \leftarrow \beta \rightarrow AUT$), tan sólo con considerar que entre AUT y SAUT (Interfaz 1) existe una *confianza explícita*, tal y como se describió en el apartado anterior.

$E = \{nSA, nAUT, AUT, SAUT\}$
$nSA \leftarrow \phi \rightarrow nAUT;$
$nSA \leftarrow \phi \rightarrow AUT;$
$AUT \leftarrow \alpha \rightarrow SAUT;$ *(interfaz 1)*

if $(nSA \leftarrow \alpha \rightarrow SAUT)$
then $(nSA \leftarrow \beta \rightarrow AUT);$ *(interfaz 6)*

La representación de esta última circunstancia queda ilustrada en la Figura 3.14, que puede entenderse como una vista parcial del Modelo de Confianza Extendido.

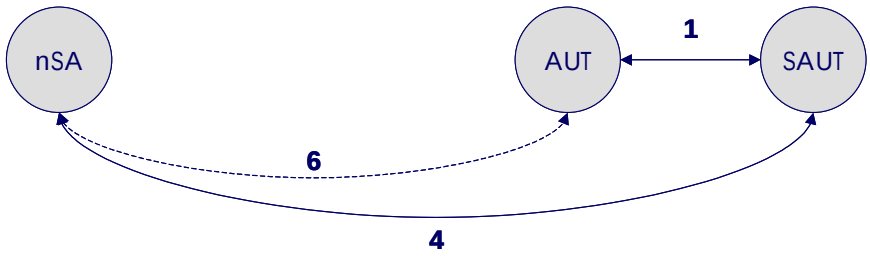

Figura 3.14 Relación de Confianza en la Interfaz 6, según el Modelo Extendido de Autenticación

Interfaz 6. La relación de confianza entre el DS (nSA) y el punto o servidor de acceso a la red, PA (AUT) (Figura 3.14) es considerada como de *confianza implícita* siempre y cuando la *confianza explícita* en la Interfaz 1 esté garantizada según se ha descrito previamente, y en la Interfaz 4 se hayan provisto protocolos y mecanismos acordes con el Modelo Extendido de Autenticación y los requisitos asociados.

Tras este análisis de las relaciones de confianza sobre las entidades pertenecientes al Modelo Extendido de Autenticación conseguimos establecer las condiciones para dotar de un valor de *confianza implícita* a la interfaz entre los dispositivos DS y EU, habiendo partido de la premisa inicial que los consideraba *no confiables*.

Como consecuencia de este Modelo de Confianza Extendido que aquí se propone, se podría derivar un impacto no sólo en aspectos tecnológicos, objeto de nuestro estudio, sino que, más allá, podría ocasionarlo también en el modelo de negocio. Este último hecho tendría su justificación en tanto que el servidor de autenticación AAA encargado de la autenticación del terminal EU podría pertenecer a un dominio administrativo distinto al encargado de autenticar el dispositivo DS. Por tanto, técnicas basadas en servidores intermediarios (p.e. *proxies* AAA) y los adecuados acuerdos y políticas de *roaming* e interconexión, podrían tener cobijarse al amparo del Modelo de Confianza Extendido aquí propuesto.

3.5.2. Generalización del Modelo de Confianza Extendido

El Modelo de Confianza Extendido merece una consideración adicional relativa a la *propiedad de anidamiento*, cuya aplicación se traduciría en una generalización del mismo. Con interés tangencial en nuestro trabajo, quede constancia de este hecho por sus posibles repercusiones futuras.

Sea un esquema de autenticación E basado en el Modelo Extendido de Autenticación y regido por los Requisitos de Autenticación enunciados, donde se incorpora una entidad n-ésima como nueva solicitante de autenticación, nSA_n, y consecuentemente una nueva entidad implementa la funcionalidad de autenticador, $nAUT_n$. Obsérvese que $nAUT_1$ se

corresponde con SA. Debe entenderse el valor de n como el *número de anidamientos* en el Modelo de Confianza Extendido.

$$E = \{nSA_n, nAUT_n, \ldots nSA_1, SA, AUT, SAUT\}$$
$$para\ n = 1, 2, 3\ldots$$

según nuestro Modelo de Confianza Extendido podemos afirmar que,

$$\exists I_i\ como\ interfaz\ entre\ nSA_n\ y\ nAUT_n$$
$$para\ I_0 = I_3\ e\ I_{i+1} = I_{i+(n+1)}\ donde\ n = 1,2,3\ldots$$
$$tal\ que\ (nSA_n \leftarrow \beta \rightarrow nAU_n)$$

Dicha afirmación se puede demostrar de la siguiente manera:

$$E = \{nSA_n, nAUT_n, \ldots, SAUT\}$$
$$(nSA_n \leftarrow \phi \rightarrow nAUT_n);$$

$$if\ (nAUT_n \leftarrow \alpha \rightarrow SAUT) \qquad (interfaz\ I_e)$$
$$\&\&\ (nSA_n \leftarrow \alpha \rightarrow SAUT) \qquad (interfaz\ I_x)$$

$$then\ (nSA_n \leftarrow \beta \rightarrow nAUT_n); \qquad (interfaz\ I_i)$$

en donde las interfaces I_e e I_x son de *confianza explícita*, según nuestro modelo, y se pueden expresar como:

$$I_e = I_{i-1}$$
$$I_x = I_{i-(n+2)}$$

Consecuentemente, la entidad nSA_n establecerá un conjunto de relaciones de *confianza implícita* con otras entidades pertenecientes al mismo esquema de autenticación E. La identificación de dichos interfaces, I_m, viene dada por las siguiente expresión para cada I_i,

$$I_m = I_{i+k}\ para\ k = 1,2,..n$$

Para la mejor comprensión de la propiedad de anidamiento del Modelo de Confianza Extendido téngase en cuenta el siguiente ejemplo. Tomando como referencia el modelo de la Figura 3.11, un anidamiento del modelo con valor n=3 supondría,

Sea $E = \{nSA_3, nAUT_3,...,nSA_1, SA, AUT, SAUT\}$

Si $\exists I_x = I_7$ *como interfaz entre* $nAUT_3$ *y* $SAUT$
tal que $(nAUT_3 \leftarrow \alpha \rightarrow SAUT)$
y $\exists I_e = I_{11}$ *como interfaz entre* nSA_3 *y* $SAUT$
tal que $(nSA_3 \leftarrow \alpha \rightarrow SAUT)$
entonces $\exists I_i = I_{12}$ *como interfaz entre* nSA_3 *y* $nAUT_3$
tal que $(nSA_3 \leftarrow \beta \rightarrow nAUT_3)$,
$\exists I_m = I_{13}, I_{14}, I_{15}$ *interfaces con* nSA_1, *SA, AUT*
tal que $(nSA_3 \leftarrow \beta \rightarrow nSA_1$, *SA, AUT)*

El ejemplo analizado queda ilustrado en la Figura 3.15, en donde se destacan en sombreado las entidades extremo, participantes en un determinado proceso de autenticación al introducir un nuevo dispositivo solicitante. Otras relaciones de confianza establecidas previamente no han sido representadas por claridad en esta ilustración.

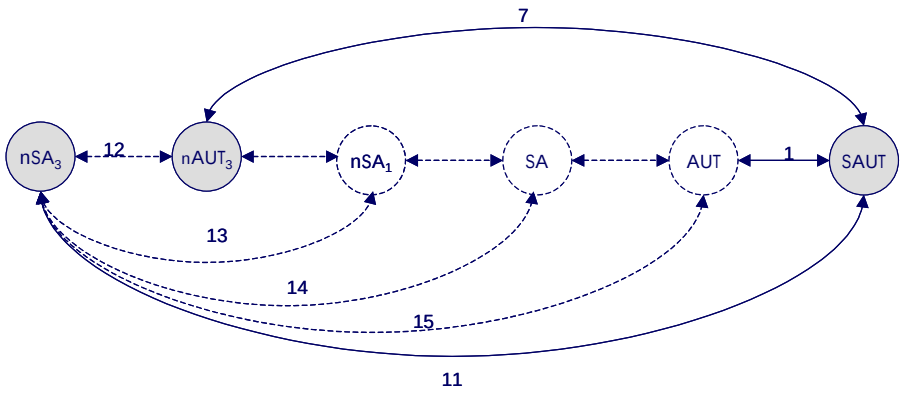

Figura 3.15 Ejemplo de Modelo de Confianza Extendido con anidamiento n=3

Sobre la base de lo expuesto en este epígrafe la definición del modelo propuesto en la Figura 3.11 como foco de nuestro trabajo podría generalizarse bajo el concepto de Modelo de Confianza Extendido con anidamiento n =1. En cualquier caso, será éste último el de máximo interés en esta tesis, dado que para valores de n>1 podría ser aplicable a una multitud de dispositivos, pero difícilmente para tarjetas inteligentes, salvo en el caso en el que ésta adoptara la funcionalidad nSA_n , donde n toma su valor máximo.

Una arquitectura de protocolos que responda al Modelo Extendido de Autenticación y cumpla con los Requisitos de Autenticación, vería representadas las relaciones de confianza entre las entidades participantes en el Modelo de Confianza Extendido *ad hoc*. En este sentido, se define en la siguiente sección una nueva arquitectura aplicable en escenarios en los que la entidad nSA del Modelo Extendido de Autenticación es una tarjeta inteligente.

3.6. Nueva Arquitectura de Protocolos de Autenticación Remota para Tarjetas Inteligentes

Una nueva arquitectura de protocolos concreta se hace necesaria, en respuesta al Modelo Extendido de Autenticación, en el que el dispositivo DS (nsA) es implementado por una tarjeta inteligente. Dadas las ventajas que presenta el protocolo *Extensible Authentication Protocol*, EAP [Abo04] un estudio detallado de sus características nos permitirá demostrar la conveniencia de su utilización como protocolo estandarizado. El objetivo es integrarlo de forma transparente respetando los Requisitos de Autenticación enunciados y, en especial, minimizar el impacto que esto supone, en los términos que requiere el requisito 6, *R6*.

3.6.1. Marco de Trabajo de Autenticación, EAP

EAP (Extensible Authentication Protocol) es un marco de trabajo para la autenticación (authentication framework), que queda recogido en el RFC 3748 con la categoría de "*Standard Track"* (*R6*). Por tanto, EAP no es un método de autenticación en sí mismo sino un soporte para múltiples Métodos de Autenticación (EAP method Types), propiamente dichos. Como ejemplo ya referenciado, el protocolo TLS proporcionaría un servicio de autenticación basado en certificados digitales y da lugar al protocolo EAP-TLS [Abo99]. En este caso, EAP acuerda el protocolo de autenticación a hacer uso entre los extremos y transporta los paquetes TLS. El servicio de autenticación, propiamente dicho, es proporcionado por TLS, conforme a sus especificaciones.

EAP fue diseñado para su uso en autenticación para acceso a redes, sin requerir conectividad en capa IP. Así, no se trata de un protocolo de transporte de datos, sino de una arquitectura para transportar paquetes de protocolos de autenticación. Típicamente

corre sobre la capa de enlace tal como PPP [Sim94] (líneas dedicadas, conmutación de circuitos, líneas dial-up, etc.) o IEEE 802 (conmutadores Ethernet, puntos de acceso inalámbricos, etc.) sin requerir conectividad IP (*R2*). Conviene señalar aquí que la encapsulación en tramas de tipo ethernet (redes locales cableadas) queda descrita en [802.1X] mientras que la encapsulación en redes locales inalámbricas queda recogida en [802.11i].

EAP es un protocolo de "un paso con bloqueo" (lock-step) por lo que un solo paquete puede estar en tránsito en cualquiera de los dos sentidos de la comunicación. (request-response). Parte de la nomenclatura utilizada en éste estándar es tomada de la nomenclatura establecida en IEEE 802.1X; por tanto, EAP considera también las tres entidades en el proceso de autenticación, definidas previamente. Así, encontramos el solicitante de autenticación (*supplicant*) como entidad que responde al autenticador (*authenticator*), siendo ésta última la entidad que inicia la autenticación con un mensaje EAP. El autenticador puede actuar en modo *pass-through* (p.e. un servidor de acceso a red o *NAS*) o como servidor de autenticación EAP, si incluye dicha funcionalidad. Finalmente, el servidor de autenticación EAP -propiamente dicho-, también nombrado como servidor AAA (*backend authenticaton server* o *AAA server*), proporciona un servicio de autenticación al autenticador. Dicha entidad ejecuta los métodos EAP para el autenticador. Como se ha mencionado, el Método EAP es el protocolo de autenticación, propiamente dicho, que implementa los algoritmos y mecanismos de autenticación, mientras que el marco EAP permite, entre otras facilidades, el transporte de los mensajes de autenticación necesarios para hacer aquellos posibles.

La características más relevantes del marco de trabajo EAP son a continuación descritas; esto nos permitirá identificar a lo largo de los próximos párrafos en qué medida éste cumple con los requisitos enunciados en nuestro trabajo y, por tanto, la viabilidad de su consideración para la proposición de una arquitectura sobre la base del Modelo Extendido de Autenticación Remota.

Flexibilidad: permite seleccionar un mecanismo de autenticación específico para el solicitante (*Supplicant*) a petición del autenticador (*Authenticator*). De otro lado, gracias a este protocolo es posible solicitar al autenticador que se actualice incluyendo un nuevo método de autenticación. Al mismo tiempo, permite al servidor de autenticación que implemente diversos métodos EAP de autenticación.

Múltiples mecanismos de autenticación: partiendo de un conjunto de ellos disponibles, es posible acordar entre los extremos el uso de uno en concreto, sin la necesidad de negociar con antelación uno en particular (*R4*). El autenticador, bajo su funcionalidad *pass-through* (p.e. un servidor de acceso a red o NAS), que no tendría por qué entender cada método de autenticación.

Separación de las funcionalidades de autenticador y del servidor de autenticación: simplifica la gestión de los credenciales y la realización de políticas de decisión, aunque este aspecto complica el análisis de seguridad y la distribución de claves (si fuera necesaria), facilita la escalabilidad (*R5*).

Secuencia de métodos de autenticación: EAP no soporta múltiples métodos de autenticación en la misma conversación pero sí soporta estos métodos de forma secuencial. El mejor ejemplo: método *Identidad* y luego *Desafío- MD5*.

Mecanismos de túnel: aunque EAP no soporta múltiples métodos de autenticación en una misma conversación, soporta mecanismos de túnel; es decir, la posibilidad de encapsular un método de autenticación dentro de otro (p.e. EAP-TTLS [Fun06]).

En definitiva, gracias a EAP es posible negociar un método de autenticación extremo-a-extremo en el que hay tres entidades involucradas. Después del adecuado intercambio de mensajes EAP se logrará una autenticación exitosa y por tanto el autenticador decide permitir el acceso al solicitante (*supplicant*) y éste está en disposición de hacer uso de dicho acceso. La decisión del servidor de autenticación, típicamente, considera aspectos de autenticación, autorización y *accounting*. EAP puede garantizar la mutua autenticación (*R2*), en caso de que el Método EAP elegido así lo haga; pudiera darse la circunstancia de que el solicitante autenticara al autenticador, pero éste niegue el acceso al primero basándose en razones de políticas de acceso.

Adicionalmente, EAP incorpora los mecanismos de retransmisión, siendo en las capas inferiores donde se garantiza el orden en la transmisión (*ordering guarantees*), y la detección de duplicado (*duplicate elimination*). Esto nos obligará a prestar especial atención a los protocolo de capas inferiores.

Sin embargo, no incorpora mecanismos de fragmentación y reemsamblado, por tanto estos mecanismos deben ser incorporados por los propios métodos de autenticación. Por estas razones, el uso de EAP está especialmente recomendado en casos en los que las capas inferiores no presenten un tasa alta de pérdidas de paquetes (tanto en el enlace DS-EU como en el EU-SAUT), que obligaría a un elevado número de *round-trips*.

Por defecto, en RFC 3748 se recogen 4 posibles Métodos (tipos) de autenticación EAP, aunque otros pueden ser añadidos, según los tipos (*types*) expandidos y numerados de 7 a 254: Identidad, Desafío-MD5, contraseña de único uso (*one-time password* o OTP) y el basado en dispositivo hardware de seguridad (*generic token card* o GTC).

Por otra parte, las posibilidades de transporte de EAP dentro de mensajes del protocolo RADIUS según el estándar [Abo03], nos permitiría aprovechar las ventajas de éste como mecanismo para establecer una autenticación mutua basada en secreto compartido entre las entidades AUT y AAA, tal como requiere el requisito *R3*.

Como se ha demostrado a lo largo de esta sección, las propiedades EAP le hace merecedor de ser un candidato adecuado como marco de trabajo para la pretendida arquitectura de protocolos de autenticación basada en el Modelo Extendido de Autenticación y respetuosa con los requisitos enunciados.

Sin embargo, es importante observar que cuando se considera una tarjeta inteligente como dispositivo DS, el requisito *R1*, relativo a la independencia de éste en el proceso de autenticación (*self-authenticable*), no viene resuelto directamente por la consideración de EAP como protocolo de referencia y esto nos obliga a focalizar el estudio del comportamiento del protocolo EAP en las tarjetas inteligentes. En la siguiente sección, se profundiza en este estudio y se propone un nuevo modelo que junto con el anterior permitirán dirigir nuestros pasos hacia una arquitectura de protocolos de autenticación coherente y robusta.

3.6.2. Nuevo Modelo de Multiplexación de EAP para Tarjetas Inteligentes

Con el objeto de dar cumplimiento a los Requisitos de Autenticación, asociados al Modelo Extendido, y en especial a *R1*, se hace necesario en nuestra propuesta incluir la definición de un nuevo Modelo de Multiplexación EAP [Abo04] aplicado a tarjetas inteligentes, en tanto que otros trabajos previos [Uri06] [SCP04], ya discutidos en esta tesis, no cumplen rigurosamente con el mismo.

El modelo que proponemos está representado en la Figura 3.16. Es destacable en este punto, que dicho modelo sería válido y aplicable tanto para las actuales tarjetas del tipo ISO7816 como para su futura versión en red (*Network Smart Card*).

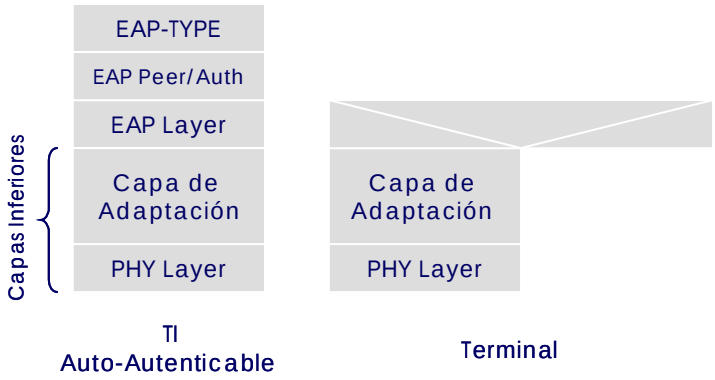

Figura 3.16 Nuevo Modelo de Multiplexación EAP para tarjetas inteligentes

El modelo ilustrado en la Figura 3.16 es una representación genérica que incide en la perspectiva de la tarjeta y por tanto deja abierta la posible implementación que debería llevarse a cabo en la parte del terminal. Es necesario destacar este hecho porque, para dar cuenta del Modelo Extendido de Autenticación en el que debería basarse la pretendida arquitectura de protocolos, habrá que prestar especial atención al diseño que se realice en este dispositivo con el objeto de mantener la coherencia entre ambos modelos y, por tanto, la robustez de la arquitectura final.

Nuestra propuesta, presentada como contribución en [Tor06a] parte de la idea de considerar la tarjeta inteligente como un solicitante de autenticacion no dividido, que da cumplimiento de las condiciones de atomicidad en el diseño y *auto-autenticabilidad* exigidas por él. Por tanto, no están previstas aquí funcionalidades de autenticación llevadas a cabo con la dependencia (*split-supplicant*) entre ambas entidades: tarjeta inteligente y terminal, considerado este último *a priori* no confiable.

La capa EAP mostrada en la Figura 3.16 debe ser implementada independientemente en la tarjeta inteligente, la cual aspira a participar de la manera más autónoma posible en el

proceso de acceso autenticado; de esta manera, logra ser un tarjeta inteligente *autenticable* por si misma (*self-authenticable smart card*) sin la dependencia en este proceso de otros dispositivos. Por simplicidad, nótese que sólo se ha representado la capa *EAP Peer* (no se ha representado la capa *EAP Authenticator*), en el lado del solicitante de la autenticación (*Supplicant*) y que esto no excluye la mutua autenticación, puesto que este servicio podría ser implementado por un método EAP (por ejemplo, EAP-TLS, donde un dispositivo final siempre actúa en el rol de *Peer* y el otro extremo en el de servidor de autenticación).

La capa EAP (*EAP Layer*) deberá intercambiar paquetes a través de las capas superiores e inferiores. Esta capa implementa control de duplicidad y retransmisión. Basado en el *Code Field* del paquete EAP, esta capa demultiplexa los paquetes recibidos y los entrega a la capa *EAP Peer*. Ninguno de los modelos referidos (Figuras 2.13 y 2.14) considera la ubicación de la capa EAP en la tarjeta inteligente. En nuestra opinión, con el objeto de dotar de autonomía en el proceso de autenticación y fortalecer la seguridad del sistema, la integración de tal capa en la tarjeta inteligente es necesaria independientemente de otros dispositivos o mecanismos.

A diferencia del modelo en la Figura 2.13 la capa *EAP Peer* debería estar localizada en la tarjeta inteligente por las mismas razones indicadas más arriba. Así, la interfaz de tarjeta inteligente no es necesaria en los términos descritos en [Uri06]. La capa *EAP Peer* demultiplexa los paquetes recibidos desde la capa EAP y, de acuerdo con el campo de tipo *Type Field* , estos paquetes son entregados al método EAP identificado en tal campo. En contraste con el modelo presentado en la Figura 2.14, no es necesario definir un marco de trabajo del tipo UICC EAP, en tanto que las capas *EAP Peer* y *EAP Layer* se proporcionan directamente servicios entre ellas, *dentro* de la propia tarjeta.

Del mismo modo que en los modelos referidos (Figuras 2.13 y 2.14), en nuestra propuesta el/los método/s EAP están localizados en la tarjeta inteligente y podrían ser implementados como un aplicación cliente. Esta capa intercambia directamente los paquetes EAP con la capa *EAP Peer*. Los métodos EAP son responsables de los algoritmos de autenticación propios de la tarjeta inteligente, así como de la fragmentación y reensamblado acorde con la interfaz física de comunicaciones.

Más allá de las diferencias identificadas y las ventajas que aporta el modelo de la Figura 3.16 para los objetivos de esta tesis, resulta interesante analizar las posibilidades de diseño en el terminal. Así, nuestro modelo, aún cuando cumple con *R1*, abre la posibilidad que el terminal adopte o no funcionalidades de autenticación dentro del esquema global. Sin embargo, la necesidad de mantener la coherencia con el Modelo Extendido de Autenticación en el que basamos este trabajo dicho terminal deberá proporcionar acceso de la tarjeta inteligente al resto de la red y, adicionalmente, participar en el proceso de autenticación en el rol de autenticador (AUT), en los términos que se viene explicando. Este hecho refuerza el concepto por el que se apuesta en esta tesis de *non-split supplicant*, en tanto que bajo esta condición el terminal no podría actuar de solicitante y autenticador para una misma entidad nSA, obligando a la clara separación de funcionalidades entre la tarjeta inteligente y éste. Hacemos notar las ventajas que esto supone en aras de garantizar la seguridad del esquema completo. Al mismo tiempo, el nuevo Modelo de Multiplexación EAP para tarjetas inteligentes y en harmonía con el Modelo Extendido de Autenticación propuesto, permiten mantener las funcionalidades genéricas previstas en el servidor de autenticación (SAUT) sin

modificación alguna. De otro lado, otros mecanismos de seguridad involucrados en las capas inferiores -excluidos del modelo y de nuestro trabajo- entre ambos dispositivos deberían ser proporcionados con el fin de establecer un servicio de autenticación más robusto.

Una vez realizada la descripción de este nuevo modelo, sobre el que descansa el concepto de tarjetas inteligentes auto-autenticables en el contexto de esta tesis, especificamos en detalle en la próxima sección una posible Capa de Adaptación, representada en la Figura 3.16, con el objeto de estudiar la factibilidad de su implementación

3.6.3. Capa de Adaptación

Este nuevo modelo plantea unos retos desde el punto de vista de la implementación y que son asumidos dentro de nuestro trabajo, proponiendo una vía de solución basada en las características propicias del protocolo PPP.

Como se ha mencionado previamente, la especificación original de la IETF del protocolo EAP (en particular de la capa *EAP Layer*) fue concebido para ser implementado sobre capas de enlaces como las basadas en el protocolo PPP y posteriormente extendida para soportar IEEE 802.1X. Actualmente, otros borradores de Internet están siendo desarrollados con el fin de implementar EAP sobre distintos protocolos (p.e. IKEv2). Sin embargo, no existe ninguna especificación o recomendación sobre cómo hacerlo sobre la pila de protocolos ISO7816 de la tarjeta inteligente. Este es uno de los desafíos de la implementación de nuestro modelo, sobre todo cuando diferentes tecnologías de capa física podrían hacer uso de una única capa de enlace. La solución sobre la se trabajará en esta tesis descansa sobre una capa de adaptación denominada Capa de Enlace Adaptada (*Adapted Link Layer*), Figura 3.16, la cual soporta un subconjunto de funcionalidades importadas desde el protocolo PPP [Sim94]. En cualquier caso, ha de notarse que el modelo propuesto ante la inclusión de esta capa de adaptación basada en PPP, sigue siendo coherente con la concepción de una tarjeta en red bajo el concepto *Network Smart Card*; de esta forma queda reforzada la elección de PPP como protocolo objetivo.

La elección de dicho protocolo está basada en las siguientes consideraciones. PPP es un protocolo ampliamente conocido y estandarizado también por la IETF. Podría proporcionar un espectro de servicios, una vez que se dispone de conectividad en la capa de enlace, ya que permite el encapsulado de datagramas de distintos protocolos que podrían incorporarse con propósitos adicionales. Nuestra implementación aprovecha las funcionalidades del protocolo LCP previstas en PPP y de la versatilidad en la autenticación que presenta, gracias a las extensiones, y en concreto, a través del protocolo EAP, *Extensible Authentication Protocol.* Las funcionalidades referidas al control de red incluidas en el subprotocolo NCP, en principio, permanecen fuera del alcance de este trabajo. Sin embargo, conviene notar que la implementación de un protocolo de capa 2 (según OSI) en la tarjeta inteligente es totalmente coherente con el resultado de los análisis previos descritos a lo largo de este documento.

Dado la naturaleza de EAP, éste se ajusta adecuadamente a las características del protocolo PPP y parece razonable implementar este protocolo en la capa de enlace con el objeto de absorber las diferencias y dificultades sólo en uno de los lados de la interfaz, es decir las capas inferiores de la tarjeta inteligente. Una ventaja adicional es que PPP no requiere de un identificador de interfaz universal, y permite una fácil integración. Adicionalmente, el protocolo PPP es capaz de trabajar con capas físicas que operan en modo síncrono o modo asíncrono. Aunque hay, y habrá, una variedad de tecnologías a emplear en esta capa de la tarjeta inteligente, las más aceptadas hasta el momento permiten la comunicación asíncrona *full/half duplex* con diferentes tasas de transmisión. Por tanto, PPP se ajusta también a estas características. En relación a los detalles de fragmentación, con PPP podríamos adaptar el MRU (*Maximum Receive Unit*) a distintos tamaños, incluyendo los tamaños reducidos, requeridos habitualmente tanto en las tarjetas de contacto como en las de *sin contacto*.

El Modelo Extendido de Autenticación, el Modelo de Confianza Extendido y el Modelo de Multiplexación EAP para tarjetas inteligentes, junto con la formalización de los Requisitos de Autenticación, conforman una parte de nuestro nuevo Marco de Autenticación para tarjetas inteligentes, a falta de la arquitectura de protocolos que se detalla en el próximo epígrafe.

Una vez definida una pila de protocolos para la tarjeta inteligente coherente respecto a nuestra propuesta, procedemos con la concepción de una arquitectura completa en la que la integración de dicha pila, y por ende de la tarjeta, resulte robusta y represente una solución como esquema de autenticación remota.

3.6.4. Arquitectura de Protocolos de Autenticación Remota para Tarjetas Inteligentes

La concepción de una Arquitectura de Protocolos de Autenticación Remota para tarjetas inteligentes, debe aspirar a cubrir con las máximas garantías de seguridad los procesos de autenticación de forma conjunta; para ello, responderá a los modelos y los requisitos que se han definido previamente. Como se describe en los apartados anteriores, de la integración de este dispositivo como solicitante de autenticación, SA, sobre un escenario que responda al Modelo Genérico de Autenticación, se han derivado consecuencias relativas a los protocolos de autenticación a implementar. Tales protocolos deberán estar en consonancia con los modelos aquí propuestos y que albergan esta nueva circunstancia: Modelo Extendido de Autenticación y Modelo de Multiplexación EAP para tarjetas inteligentes.

En la Figura 3.17, se representa una Arquitectura de Protocolos de Autenticación Remota para tarjetas inteligentes respetuosa con estas circunstancias y con el objetivo último de garantizar la seguridad y robustez de tales procedimientos; de otro lado, esta arquitectura aprovecha las capacidades de las tarjetas inteligentes ISO 7816 como, entre otras, la de implementar protocolos de capa 2, así como, las de procesado y almacén seguro.

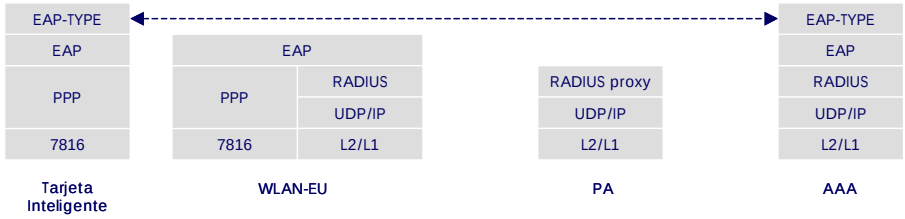

Figura 3.17 Arquitectura de Protocolos de Autenticación Remota para Tarjetas Inteligentes

Nótese, no sólo que la funcionalidad de solicitante de autenticación está netamente implementada en la tarjeta inteligente, sino que además el EU participa como un *servidor o punto de acceso* implementando el rol autenticador según [Abo03]. Esto supone que, una vez que PA y EU han sido correctamente autenticados por AAA, es posible *desplazar* la funcionalidad de autenticador desde PA, en donde residía según la concepción tradicional, hasta EU. En esta fase por tanto, el PA de nuestra arquitectura tomaría la funcionalidad de proxy RADIUS y podría localizarse en el acceso de la red local, con el objeto de participar en el proceso de autenticación de la tarjeta inteligente.

En un enfoque opcional al presentado, el PA podría mantener su funcionalidad de autenticador, convirtiéndose el EU en un elemento netamente de *relay*. En dicho caso, el PA como autenticador podría ser el mismo que diera servicio de autenticación a los EUs registrados en la misma red local; unas políticas de seguridad adecuadas deben considerarse, en tanto que, podrían permanecer a distintos dominios –TI y EU-, y por ende dispondrían de distintos servidores de autenticación AAA. Este enfoque aquí sugerido, se discutirá como posible futuro trabajo.

Esta arquitectura prevé una tarjeta inteligente, TI, autónoma en el proceso de autenticación mutua extremo-a-extremo entre ésta y el servidor de autenticación, y que debería ser independiente al procedimiento por el cual el usuario introduce el PIN para autenticarse frente al sistema. Por tanto, aquella podría ser considerada como una autenticación para el acceso a la red de un dispositivo, basada en las credenciales propias de éste. A continuación se analiza la capacidad de la tarjeta inteligente para con el cumplimiento de los Requisitos de Autenticación, definidos en 3.3.1.

En relación a *R1*, y como se ha demostrado en el punto anterior, la implementación del Modelo de Multiplexación EAP propuesto se hace indispensable. Más allá, la tarjeta TI debe proporcionar sus propios credenciales de seguridad y estos deben ser diferentes de los del usuario y del terminal EU. Dichos credenciales deben ser inaccesibles mediante cualquier método software o hardware, para lo que la pretendida condición de *tamper resistant* la hace altamente efectiva.

De otro lado dadas las ventajas que el protocolo EAP, así implementado, ofrece, se garantiza un esquema de autenticación mutua extremo-a-extremo, tal como prevé el

requisito 2 (*R2*), ante un servidor de autenticación remoto, sobre una arquitectura que podría ser heterogénea. Por tanto, el proceso de autenticación se realiza entre dispositivos independientes (y la tarjeta como uno de ellos) durante el procedimiento de acceso a redes, haciendo posible la conectividad en capa 2 sin la necesidad expresa de que la tarjeta inteligente implemente al completo la pila de protocolos TCP/IP, lo cual representa una clara ventaja. Por tanto, en este sentido podríamos decir que la tarjeta inteligente está integrada en el sistema como un dispositivo de red en el plano de la autenticación, comparable a cualquier nodo de la red, sin disponer de una capa 3 (según OSI) como tal. Además de ésta, son otras las ventajas de autenticación a este nivel. La implementación de protocolos de autenticación en capa 2, no excluye la posibilidad de hacerlo en capas superiores en caso de ser necesario y posible. Por tanto, la integración de estos protocolos debería no sólo no ser un impedimento para la implementación de capas de red en la tarjeta inteligente, sino que más allá, debería facilitarlo.

El cumplimiento del requisito de mutua autenticación, *R2*, queda justificado ante el hecho de que un ataque en este contexto podría ser visto tanto desde la perspectiva de la tarjeta inteligente, TI, como desde la del servidor de autenticación, AAA. Por tanto, en la Arquitectura de Protocolos de Autenticación Remota la tarjeta inteligente debe ser capaz de implementar funcionalidades tanto de solicitante de autenticación (*peer* o *supplicant*) como de autenticador (authenticator). De esta forma, se evitaría que el servidor pudiera ser suplantado con el objeto de obtener información crítica sobre la tarjeta inteligente o proporcionar un servicio de forma maliciosa. Por lo tanto, el servidor debería ser correctamente autenticado por la tarjeta inteligente. De otro lado, una tarjeta no autenticada podría ser falsificada (sus credenciales) con intenciones maliciosas. Tradicionalmente, en los procesos de autenticación con tarjetas inteligentes, se ha puesto mayor énfasis en la autenticación en el lado del usuario, bajo una visión quizás algo denostada en la que el origen de irregularidades se centrarían en dicho elemento, olvidando la posibilidad de que éste fuera la auténtica víctima frente a un terminal o sistema malintencionado.

Son múltiples los métodos EAP que permiten la mutua autenticación. En cualquier caso, esquemas ligeros de reto-respuesta aplicado en ambos sentidos permitiría llevar a cabo la mutua autenticación sobre la arquitectura propuesta. Son diversos los métodos EAP que implementan mecanismos para el establecimiento de claves de sesión y que garantizan el refresco de las mismas. Conviene señalar aquí, que las técnicas de autenticación mutua entre el terminal y la tarjeta, basadas en los comandos ISO7816 (INTERNAL AUTHENTICATE), no son objeto directo de nuestro trabajo, por tratarse de un enfoque local entre dispositivos y no considera la tarjeta como integrante de un sistema de red, en el sentido entendido en esta tesis.

De otro lado y dando cumplimiento al requisito, *R4*, la definición de una arquitectura de protocolos de autenticación para tarjetas inteligentes debería ser definido en la manera y modo que permitiera que ésta pudiera participar durante el procedimiento de autenticación, en procesos de acuerdo o negociación segura y flexible del conjunto de mecanismos y de algoritmos de cifrado de entre los disponibles. En el caso de trabajar con tarjetas inteligentes actuales, este requisito pude verse limitado, aunque no excluido, por la propia naturaleza de la tarjeta tanto por su capacidad de comunicación como en la de procesado. Sin embargo, el abanico de posibilidades que se despliega a partir de la implementación de EAP en el conjunto de la arquitectura, permite ajustar la

complejidad del mecanismo o algoritmo a emplear, dependiendo de cada contexto en los que participa la tarjeta inteligente.

En relación a la capacidad escalable de la gestión de las claves, R5, en la concepción de esta arquitectura para tarjetas inteligente, el impacto no es tanto en el servidor de autenticación, como lo pudiera ser en la tarjeta inteligente. Así, las tarjetas inteligentes multi-aplicación registradas en diferentes redes podrán cumplir con este requisito de escalabilidad hasta donde su capacidad se lo permita. La implementación de distintos tipos de métodos EAP en la misma tarjeta para distintas aplicaciones, por ejemplo, permiten una gestión de claves adecuada.

En cuanto al requisito *R6,* se dio cuenta de la condición de EAP y PPP como protocolos estandarizados, garantizando su solvencia en multitud de contextos y en interoperación con otros protocolos igualmente reconocidos.

Referente al cumplimiento del requisito *R3* en la arquitectura propuesta, podrá encontrarse justificación detallada en el siguiente punto.

Análisis de la Seguridad de la Arquitectura de Protocolos de Autenticación Remota

Procedemos en este apartado un análisis de la seguridad de la arquitectura propuesta a partir de las relaciones de confianza que se establecen entre las entidades participantes. Para el desarrollo de éste, conviene comenzar por el estudio parcial dicha arquitectura.

Consideremos en primer lugar, la parte de la arquitectura que se encarga de la autenticación del terminal EU, previamente a la inclusión de la tarjeta TI en el esquema, Figura 3.18. En esta fase (Fase 1) se verían involucrados los interfaces 1, 2 y 3 del Modelo de Confianza Extendido (coincidentes con la versión genérica de mismo). La fortaleza de los procesos de autenticación en la Interfaz 1 (PA−AAA), y al mismo tiempo, el valor de la confianza entre las entidades PA y AAA dependerá netamente de la seguridad y robustez de los mecanismos por los que se establezca y distribuya (por un canal externo seguro) un secreto compartido entre ambas, tal como exige *R3*. A partir de aquí, podrían implementarse protocolos implementados sobre la base de tal secreto, RADIUS [Abo03] o DIAMETER [Ero05]. Bajo esta premisa, el valor de la relación de confianza en la interfaz PA−AAA, sería de *confianza explícita*, una vez llevada a cabo la autenticación mutua a través de uno de estos protocolos. La ventaja de hacerlo así, en pos de nuestro trabajo, radica en la posibilidad de integrar EAP sobre RADIUS. La correcta implementación de éste garantizará la seguridad del esquema. El análisis de las amenazas potenciales queda recogido en [Abo03]. La posterior autenticación extremo a extremo del dispositivo EU con el servidor AAA, se lleva a cabo mediante la implementación del protocolo EAP y alguno de los métodos de autenticación (EAP-type) de reconocida solvencia (p.e. EAP-TLS). Esto permitiría asignar un valor cualitativo a la relación de confianza en la interfaz EU−AAA de *confianza explícita*. Entre los dispositivos EU y PA, el protocolo EAP permitirá la integración con una capa inferior de naturaleza variada, pudiendo encontrar soluciones tanto para entornos cableados como inalámbricos. Como se demostró en el epígrafe 3.4.1 la *confianza implícita* entre ambos dispositivos caracterizará esta Interfaz 3 (EU−PA).

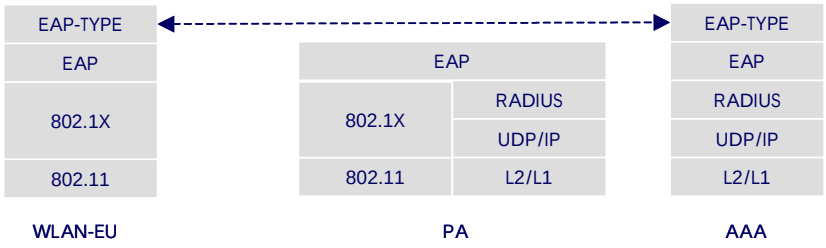

Figura 3.18 Ejemplo de Arquitectura de Protocolos de Autenticación para redes IEEE 802

Una vez resuelta esta fase inicial, el terminal EU estaría en disposición de participar en el proceso de autenticación (Fase 2) exclusivo de la tarjeta inteligente (TI), ésta última como solicitante DS y según los modelos presentados en esta tesis. Como hipótesis de partida los dispositivos TI y EU (Interfaz 5) son mutuamente *no confiables*. Tomando como base el marco de trabajo de autenticación como EAP, orientado en este sentido, se hace posible una autenticación extremo a extremo entre la tarjeta inteligente y el servidor de autenticación AAA. Siempre y cuando se atienda a una correcta implementación de los métodos de autenticación, a través de técnicas reconocidas, la capa EAP, que se extiende entre ambas entidades, así como nuestro Modelo de Multiplexación EAP aplicado a TI, podrían garantizar el cumplimiento de los requisitos de autenticación afectados y por tanto cualificar la relación de confianza en la Interfaz 6, TI-AAA, como una *confianza explícita*. Una vez conseguido este objetivo, las interfaces 5 y 6 quedarán calificadas como de *confianza implícita*, soportándose en la Interfaz 4 el peso del proceso de autenticación. Para completar esta descripción, se representa formalmente el análisis correspondiente a la arquitectura propuesta.

Fase 1:

$$E = \{EU, PA, AAA\}$$

$$(EU \leftarrow \phi \rightarrow PA);$$

$$\text{if } (PA \leftarrow \alpha \rightarrow AAA) \quad \text{(interfaz 1)}$$
$$\&\& \ (EU \leftarrow \alpha \rightarrow AAA) \quad \text{(interfaz 2)}$$

$$\text{then } (EU \leftarrow \beta \rightarrow PA); \quad \text{(interfaz 3)}$$

Fase 2:

$E = \{TI, EU, PA, AAA\}$

$(TI \leftarrow \phi \rightarrow EU);$

$(EU \leftarrow \alpha \rightarrow AAA);$

$if\ (TI \leftarrow \alpha \rightarrow AAA)$ *(interfaz 4)*

$then\ (TI \leftarrow \beta \rightarrow PA);$ *(interfaz 6)*

$(TI \leftarrow \beta \rightarrow EU);$ *(interfaz 5)*

Con la contribución en esta tesis de esta Arquitectura de Protocolos de Autenticación Remota se completa, junto con los modelos y requisitos propuestos, el nuevo Marco de Autenticación para Tarjetas Inteligentes en Red que queda detallado en el siguiente apartado. En los capítulo 4 y 5, se tratarán aspectos sobre el diseño e implementación de dicha arquitectura en lo que a la tarjeta inteligente se refiere.

3.7. Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red

El nuevo Marco de Autenticación para Tarjetas Inteligentes en Red concebido en esta tesis es el resultante de la composición del conjunto de los cinco elementos descritos en este capítulo y cuya imbricación ha sido detallada: Modelo Extendido de Autenticación, los Requisitos de Autenticación asociados, Modelo Extendido de Confianza, Modelo de Multiplexación EAP y la Arquitectura de Protocolos de Autenticación Remota para Tarjetas Inteligentes. Dicho marco pretende contemplar la autenticación de este tipo de dispositivos de una forma global, considerándolos como parte del esquema de autenticación desde las primeras fases del diseño del mismo, facilitando la integración de soluciones. Por tanto, con este nuevo marco de autenticación es posible afrontar la autenticación remota de la tarjeta inteligente simultáneamente desde distintas aristas, como un mismo problema. Aristas que engarzan lo conceptual del **modelo** con la praxis de una **arquitectura**, incorporando en todo momento el **análisis** de la seguridad basado en las relaciones de confianza.

Con la adición de este marco, se pretende facilitar la migración hacia las denominadas tarjetas inteligentes TCP/IP, o *Network Smart Card*, siendo por tanto, los componentes del Marco de Autenticación para Tarjetas Inteligentes en Red, Figura 3.19, válidos para el presente y futuro tipo de tarjetas.

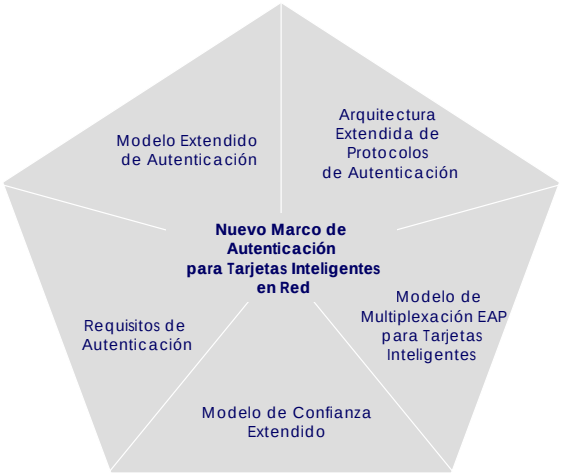

Figura 3.19 Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red

Si bien es cierto que, el presente Marco de Autenticación ha sido desarrollado para contribuir en el área de trabajos de investigación que se ocupan de la tarjeta inteligente como dispositivo de implantación masiva, con ciertas limitaciones computacionales para la comunicación y la autenticación remota, podría llevarse a cabo una generalización de mismo para abarcar una variedad de dispositivos, cuyas capacidades les permitiera una correcta y efectiva integración en la Arquitectura de Protocolos de Autenticación Remota. Este circunstancia recala en aspectos tangenciales en nuestro trabajo, tomándolos en consideración para líneas futuras.

Capítulo 4.

Diseño e Implementación bajo el nuevo Marco de Autenticación

4. Diseño e Implementación bajo el nuevo Marco de Autenticación

4.1. Objetivos del Diseño y de la Implementación

El objetivo de este capítulo es demostrar –una vez realizado el diseño correspondiente–, la viabilidad de la implementación del Marco de Autenticación definido en esta tesis, lo que nos lleva a la consideración del Modelo Extendido y en concreto del Modelo de Multiplexación EAP para tarjetas inteligentes, y su potencial integración en una Arquitectura de Protocolos como una tarjeta *auto-autenticable*, en el sentido recogido en este documento.

Para ello, se ha llevado a cabo la realización práctica de los modelos presentados en el Capítulo 3, procediendo inicialmente con una fase de diseño y posteriormente con la implementación en un entorno de laboratorio. En el Capítulo 5, se ejecutará una última fase de tests y pruebas de funcionalidades del resultado aquí obtenido. Para la fase de implementación ha sido necesaria la búsqueda de la plataforma de desarrollo más adecuada y la concepción de la metodología de pruebas que mejor se ajusta a las características de nuestro Modelo de Multiplexación EAP para tarjetas inteligentes. De esta forma, se ha procedido con la implementación que debiera desembocar en una plataforma sobre el que pudieran realizarse pruebas de distinta índole, con especial énfasis en los aspectos de seguridad de la tarjeta inteligente y su interacción con el entorno. Este objetivo está fuera del alcance de nuestro trabajo y se pospondrá a un futuro desarrollo.

4.2. Diseño del Modelo de Multiplexación EAP en la Tarjeta Inteligente

Nuestro Modelo de Multiplexación de EAP para tarjetas inteligentes quedó descrito en el epígrafe 3.6.2. En buena medida, este modelo constituye en sí mismo una pila de protocolos en torno al marco de trabajo EAP. De esta manera, el diseño del protocolo PPP por un lado, y el del protocolo EAP propiamente dicho, por otro, sobre la tarjeta inteligente según dicho modelo, van constituir el núcleo del diseño realizado en nuestro trabajo y cuyas claves se señalan en las próximas secciones.

4.2.1. Diseño del protocolo PPP en la Tarjeta Inteligente

En el Capítulo 3 de esta tesis, quedó descrita la justificación por la cual el protocolo de comunicaciones PPP [Sim94] era considerado el candidato más apropiado para implementar la *capa de adaptación* en el modelo de multiplexación, con el objeto de que sirviera de interfaz entre la comunicación basada en ISO 7816 y el marco de trabajo EAP. Por tanto, el protocolo PPP se convierte en el primer paso para hacer de la tarjeta inteligente común, una aproximación hacia las futuras tarjetas en red (Network Smart Card). Además de las razones previamente expuestas, con el diseño del protocolo PPP para la tarjeta se puede considerar la ventaja de que aquellas aplicaciones o soluciones de comunicación u otra índole basadas en la implementación resultante serán igualmente funcionales tanto para las actuales tarjetas como para las futuras. En

cualquier caso, se ha de señalar que la implementación que en este capítulo se describirá, está diseñada y posteriormente testeada, para tarjetas ISO 7816.

El protocolo PPP es uno de los protocolos más consolidados y robustos en entornos de red, que suele describirse mediante sus tres componentes esenciales: un método para encapsular datagramas de múltiples protocolos; un protocolo de control del enlace (*Link Control Protocol* , LCP) con el objeto de establecer, configurar y probar la conexión en el enlace de datos; y finalmente, una familia de protocolos de control de red (*Network Control Protocol,* NCP), para el establecimiento y configuración de diferentes protocolos de red.

El encapsulado llevado a cabo por PPP permite la multiplexación de diferentes protocolos de red simultáneamente sobre el mismo enlace. En el contexto de esta tesis, en tanto que no se registra de entre sus objetivos contemplar protocolos de red alguna, las ventajas de multiplexación que PPP ofrece no se van a ver aprovechadas, siendo por tanto las funcionalidades de encapsulado y fragmentación tangenciales en el desarrollo de este trabajo. Nótese que el reducido tamaño de los tramas a transportar sobre PPP no requerirán, como se verá más adelante, de técnicas fragmentación. Así, los protocolos de red que pudieran implementarse sobre PPP, y por tanto las funcionalidades que éste presenta mediante el protocolo NCP, no son tampoco objeto de este trabajo. Es el protocolo LCP para el establecimiento seguro del enlace el que centrará nuestros esfuerzos y sobre el que podremos diseñar en una segunda fase el protocolo EAP, objetivo final de la implementación.

El protocolo LCP es lo suficientemente versátil como para ser portable a una amplia variedad de entornos y de ello toma ventaja nuestro trabajo. Este protocolo permite no sólo iniciar y finalizar el enlace o detectar errores en éste, sino que además permite negociar o configurar el mismo mediante un intercambio de mensajes entre los dos extremos de la comunicación. La autenticación entre dichas entidades forma parte de dicho proceso de configuración.

Figura 4.1 Encapsulado en el protocolo PPP

En la Figura 4.1, queda representado el encapsulado propio de PPP. A continuación se describen algunas características de los campos que lo componen.

Campo de Protocolo puede ser de 1 o 2 octetos. identifica el tipo de datagrama que transporta una trama de PPP concreta el *Campo de Información*. Algunos protocolos interesantes son identificados mediante la codificación presentada en la Tabla 4.1. Obsérvese que dos de ellos están referidos a posibles protocolos de autenticación entre los extremos y que podrían ser negociados. Conviene señalar en este punto que la

necesidad del diseño del protocolo PPP en la tarjeta inteligente es precisamente poder proceder, conforme a estándar, con el protocolo de autenticación EAP, que ha servir para el transporte de los mensajes de autenticación sobre una red de diversa naturaleza. De entre los indicados en la Tabla 4.1, los señalados con (*) serán los de interés para nuestro diseño y que en este capítulo describimos.

Valor	Protocolo
0xC021	LCP, Link Control protocol (*)
0xC023	PAP, Password Authentication Protocol
0xC025	Link Quality Report
0xC223	CHAP, Challange Handshake Authentication Protocol
0xC227	EAP, Extensible Authentication Protocol (*)

Tabla 4.1 Opciones del Campo de Protocolo

Campo de Información contiene por tanto el datagrama del protocolo especificado en el campo anterior.

Campo de Relleno; en algunos casos podría ser necesaria un funcionalidad de relleno de la trama.

Como resumen a la descripción del protocolo PPP y para una mejor compresión del diseño llevado a cabo, en la Figura 4.2, se representa el diagrama de fases que caracteriza la configuración, mantenimiento y terminación del enlace, de las que se derivan los protocolos mencionados y que intervienen en cada caso. Quedan resaltadas las fases que han sido de nuestro interés para los propósitos de esta tesis, con especial hincapié en la fase de autenticación. Tal como se ha mencionado anteriormente, la fase de red (llevada a cabo gracias al protocolo NCP), posterior a la fase de autenticación, no es necesaria para nuestros objetivos por tanto no ha sido contemplada en este trabajo. En esta fase se negociarían los atributos del acceso a red, por ejemplo para conectividad en redes IP.

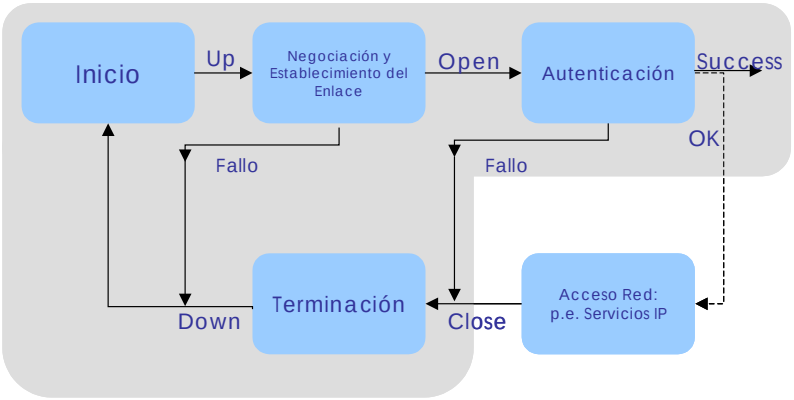

Figura 4.2 Diagrama de Fases incluidas en el diseño del protocolo PPP

4.2.2. Máquina de Estados del Protocolo PPP

Para un mejor ajuste a nuestros propósitos se ha diseñado ad-hoc una máquina de estados, simplificada respecto a la original, con la certeza de que su funcionalidad provee completamente de los servicios que requiere el protocolo EAP desde la capa inferior, al tiempo que se minimizan los recursos que un protocolo de este tipo podría llegar a consumir. Esta máquina de estados será el primer objetivo de nuestra próxima implementación en la tarjeta inteligente.

El diseño de la máquina de estados del protocolo PPP, en la fase de negociación y establecimiento del enlace, deberá servir como punto de partida de la fase de implementación. Dicho *automaton*, según se especifica en el estándar, podría llegar a ser bastante complejo, en el caso de incluir en el diseño cada una de las opciones posibles. Teniendo en cuenta que el objetivo de PPP no es más que le de facilitar la posterior implementación estandarizada del protocolo EAP en la tarjeta inteligente y demostrar así la viabilidad de nuestro Modelo de Multiplexación EAP en ésta –y por ende el Modelo Extendido de Autenticación–, sumado a las limitaciones que la misma presenta, definimos, como decisión de diseño, una versión simplificada de la máquina de estados que queda resumida en la Tabla 4.2 y cuya leyenda se recoge en la Tabla 4.3.

		Estados en la Transición							
		0	1	2	3	6	7	8	9
		Inicial	Starting	Cerrado	Parado	Petición Enviada	Confirmación Recibida	Confirmación Enviada	Abierto
Eventos	Up	2	scr/6	-	-	-	-	-	-
	Down	-	-	0	tls/1	1	1	1	tld/1
	Open	tls/1	1	scr/6	3	6	7	8	9
	Close	0	tlf/0	2	2	str/4	str/4	str/4	str/4
	RCR+	-	-	sta/2	src,sca/8	sca/8	sca,tlu/9	sca/8	tld,scr,sca/8
	RCR-	-	-	sta/2	scr,scn/6	scn/6	scn/7	scn/6	tld,scr,scn/6
	RCA	-	-	sta/2	sta/3	7	scr/6	tlu/9	tld,scr/6
	RCN	-	-	sta/2	sta/3	scr/6	scr/6	scr/8	tld,scr/6
	RTR	-	-	sta/2	sta/3	sta/6	sta/6	sta/6	tld,sta/5
	RTA	-	-	2	3	6	6	8	tld,scr/6

Tabla 4.2 Máquina de Estados simplificada de PPP

Evento	Descripción
RCR+	Recibe Petición de Configuración Válida
RCR-	Recibe Petición de Configuración Errónea
RCA	Recibe Confirmación de Configuración
RCN	Recibe No-Confirmación de Configuración
RTR	Recibe Petición de Finalizar
RTA	Recibe Confirmación para Finalizar

Acciones	Descripción
scr	Envía Petición de Configuración
sca	Envía Confirmación de Configuración
scn	Envía No-Confirmación de Configuración
str	Envía Petición de Finalizar
sta	Envía Confirmación de Finalizar
tlu	Activar esta capa
tld	Desactivar esta capa
tls	Iniciar esta capa
tlf	Finalizar esta capa

Tabla 4.3 Leyenda de la Máquina de Estados

4.2.3. Encapsulado y Mapeo de protocolos

La metodología llevada a cabo en el diseño del mapeo de tramas del protocolo PPP sobre un tarjeta ISO 7816 puede verse representada en la Figura 4.3. Se trata, en definitiva del mapeo bidireccional de cada trama original de PPP conforme al estándar, sobre una comando APDU, para el protocolo de comunicación T=0.

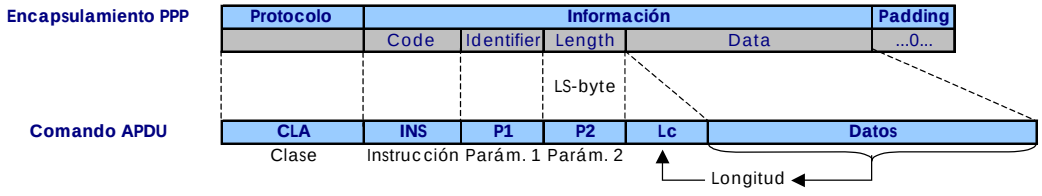

Figura 4.3 Mapeo de entre tramas de PPP y comandos APDU

En las siguiente Tablas 4.4, 4.5, 4.6, 4.7 y 4.8 se resume la interpretación de los términos que aparecen en la Figura 4.3. Aquellas opciones señaladas con (*) indican que han sido consideradas en nuestro diseño; el resto de opciones, son aquellas que quedan contempladas en los protocolos PPP y EAP, pero que no han sido incluidas, bien por su carácter de opcional o por su irrelevancia para los objetivos de demostración de nuestro desarrollo.

Campo	Descripción	Valores	Comentario
Code	Código para identificar el tipo de trama LCP	0x01--0x0B	Ver Tabla 4.5
	Código para identificar el tipo de trama EAP	0x01--0x04	Ver Tabla 4.7
Identifier	Identificador de la trama.	0--255	Control de Secuencia petición/respuesta y Duplicados
Length	Longitud campo de Informción y Relleno	0--32768	Trama completa, excepto del campo protocolo
Datos	Opciones de Configuración de LCP	Type| |Length| |Data	Ver Tabla 4.6
	Tipo de contenido de la trama EAP	Type| |Length| |Data	Ver Tabla 4.8

Tabla 4.4 Descripción de los campo de la trama PPP

Code	Tipo de Trama LCP
0x01	Configure-Request (*)
0x02	Configure-Ack (*)
0x03	Configure-Nack (*)
0x04	Configure-Reject (*)
0x05	Terminate-Request (*)
0x06	Terminate-Ack (*)
0x07	Code-Reject
0x08	Protocol-Reject
0x09	Echo-Request
0x0A	Echo-Reply
0x0B	Discard-Request

Tabla 4.5 Interpretación de los Códigos en la trama LCP

Opciones de Configuración LCP	
Type	Descripción
0x00	Reservado
0x01	MRU (*)
0x03	Protocolo de Autenticación (*)
0x04	Quality-Protocol
0x05	Magic Number
0x07	Protocol-Field-Compression
0x08	Address-and-Control-Field Compression

Tabla 4.6 Interpretación de los Tipos en la trama LCP

Codificación Trama EAP	
Code	Descripción
0x01	Request (*)
0x02	Response (*)
0x03	Success (*)
0x04	Failure (*)

Tabla 4.7 Interpretación de los Códigos en la trama EAP

Tipo de contenido trama EAP	
Type	Descripción
0x01	Identity (*)
0x02	Notification (*)
0x03	Nak (*)
0x04	MD-5 Challange
0x05	One Time Password OTP
0x06	Generic Token Card,GTC
0xFE	Tipo Extendido
0xFF	Uso experimental

Tabla 4.8 Interpretación de los Tipos en la trama EAP

Para la correcta lectura del mencionado *mapeo* se han tomado las siguientes consideraciones de diseño, que con posterioridad se verán plasmadas en la correspondiente implementación.

- El Campo de Protocolo en la trama PPP podría ser alguno de los indicados en la Tabla 4.9. El tamaño de dicho campo para dichos protocolos es de 2 bytes mientras que el tamaño del campo CLA es de 1 byte. Como, adicionalmente, por las normas de estandarización ISO7816 tal campo sólo puede tomar de entre unos valores determinados, ambas circunstancias nos obligan a codificar el campo CLA con un sólo byte, y acorde a dicha norma. Así, en el caso de este campo, el mapeo no se realiza directo sino que corresponde con una codificación, elegida como decisión de diseño propia.

Protocolo	CLA
LCP=0xc221	0xA4
EAP=0xc227	0xA0

Tabla 4.9 Mapeo entre el tipo de Protocolo y el campo CLA

- De otro lado, el campo *Length* en la trama PPP hace referencia a la longitud del Campo de Información (incluye *Code*, *Identifier* y *Length*) y al Padding (en el caso de que existiera) y se representa mediante 2 bytes, lo cual podría indicar una longitud máxima de 32Kbytes. Para el tipo de tarjeta inteligente para el que está pensada esta implementación, el tamaño máximo en el interfaz de comunicación es de 255 bytes. Esto significaría que con 1 sólo byte podríamos representar dicha longitud, y por tanto el mapeo se realizará exclusivamente con el byte menos significativo del campo *Length*. De otro lado, se ha de tener en cuenta que los mensajes a transportar en el protocolo EAP en general serían bastante inferiores a aquel tamaño, aunque particularmente esto dependerá del método de autenticación finalmente implementado. Sirva como excepción a esto, el método EAP-TLS, que por el tamaño de sus mensajes (intercambio de certificados digitales) requeriría de una estrategia de mapeo distinta, que permitiera la fragmentación y su control.

- Ha de destacarse la diferencia entre el campo *Length*, ya explicado, y el campo *Lc* (1 byte) en el comando APDU. Como se refleja en la Figura 4.3 dichos parámetros representan a longitudes distintas. Así, el valor de *Lc* no se obtiene

directamente del mapeo de alguno de los campos de la trama PPP, sino que ha de *calcularse* como medida, netamente, de la longitud del campo Datos.

Para completar esta descripción de las directrices adoptadas en la metodología de diseño, en cuanto al *mapeo* del protocolo PPP, se muestra en la Figura 4.4a un ejemplo de trama LCP para la configuración del protocolo de autenticación. En tal ejemplo, se trata del protocolo EAP, que es aceptado por la tarjeta y responde con el comando apropiado, que es debidamente mapeado en el terminal, según el protocolo estandarizado LCP (Figura 4.4b).

Protocolo	Información					
LCP	Code	Identifier	Length	Data=Configurations Options		
				Type	Length	Data
0xc221	0x01	0x01	0x0008	0x03	0x04	0xC227
	Request	Ident. 1	8 bytes	Prot. Auten.	4 bytes	EAP

CLA	INS	P1	P2	Lc	Datos			
0xA4	0x01	0x01	0x08	0x04	0x03	0x04	0xC2	0x27
	Request	Ident. 1	8 bytes	4 bytes	Prot. Auten.	4 bytes	EAP	

Figura 4.4a Ejemplo de mapeo para la configuración de la Autenticación con EAP: solicitud del terminal

CLA	INS	P1	P2	Lc	Datos				SW1	SW2
0xA4	0x02	0x01	0x08	0x04	0x03	0x04	0xC2	0x27	0x90	0x00
	Conf.-Ack	Ident. 1	8 bytes	4 bytes	Prot. Auten.	4 bytes	EAP		OK	

Protocolo	Información					
LCP	Code	Identifier	Length	Data=Configurations Options		
				Type	Length	Data
0xc221	0x02	0x01	0x0008	0x03	0x04	0xC227
	Conf.-Ack	Ident. 1	8 bytes	Prot. Auten.	4 bytes	EAP

Figura 4.4b Ejemplo de mapeo para la configuración de la Autenticación con EAP: respuesta de la tarjeta inteligente

4.2.4. Diseño del Protocolo EAP en la Tarjeta Inteligente

Como se ha visto en el punto anterior, mediante el protocolo LCP ambos extremos se ponen inicialmente de acuerdo con continuar con un proceso de autenticación basado en EAP, una vez que el enlace esta establecido y procede llevar a cabo la fase de autenticación (Figura 4.2) . A partir de este momento, en el interfaz tarjeta-terminal se intercambiaran mensajes del protocolo EAP. Para llevar a cabo este procedimiento, se ha diseñado, una versión de la máquina de estados original, que queda claramente reflejada en el diagrama de clases de dicho protocolo, recogido en las recomendaciones y especificaciones descritas en [Vol05]. Para una mejor interpretación del código a implementar, se respetará en todo momento la nomenclatura allí utilizada. El diagrama de clases completo, que ha servido como referencia de diseño, queda representado en la Figura 4.5, en la que la tarjeta inteligente, respetando nuestros modelos, ejerce el rol de nuevo solicitante de autenticación, nSA. Se ha de señalar que las técnicas de mapeo indicadas en el apartado 4.2.3 son plenamente aplicables en este caso.

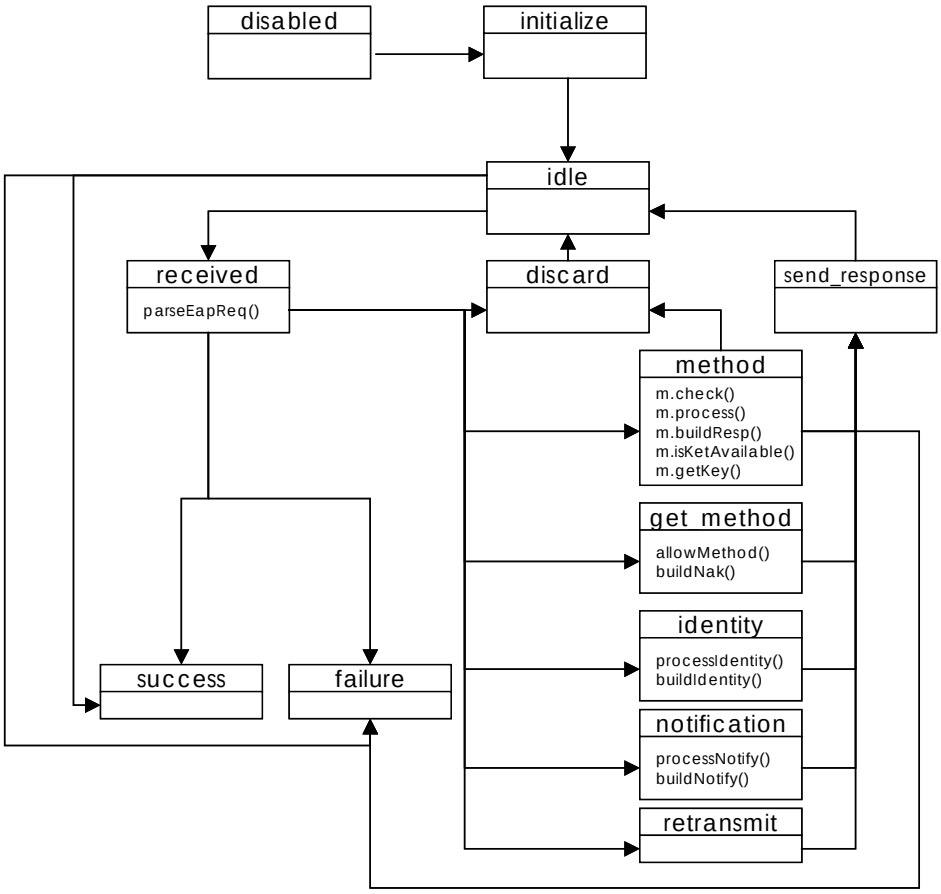

Figura 4.5 Diagrama de clases completo para la Tarjeta Inteligente auto-autenticable en el rol de nSA

Para una mejor adecuación a nuestro Modelo de Multiplexación EAP para la tarjeta inteligente (Figura 3.16) propuesto en este trabajo, el diseño del mismo en la tarjeta se realizará de forma que cada capa del protocolo corresponda a una clase distinta, permitiendo con ello dotar al diseño, y a la posterior implementación, de un valor organizativo, e incluso didáctico, que favorece su estudio y su ampliación en caso necesario.

4.3. Selección de los entornos y herramientas de implementación

Una vez realizado el diseño de los protocolos requeridos, procedemos en esta sección con el estudio del entorno y herramientas necesarios para llevar a cabo la implementación correspondiente. En este sentido, se ha seleccionado la tecnología Java Card por su potencial y ventajas que presenta, avalados por la amplia aceptación en el

sector especializado. Destacamos en este punto, la interoperabilidad de la plataforma Java y las posibilidades de desarrollo que muestra. La selección de esta tecnología, junto con el entorno de desarrollo Java Card 2.1.2 Development Kit, garantizan un resultado escalable en función de las necesidades futuras que de este trabajo pudieran derivarse.

4.3.1. Tecnología Java Card

La tecnología Java Card de Sun Microsystems adapta la plataforma Java para su utilización en tarjetas inteligentes y en otros dispositivos con una memoria y una potencia de procesamiento muy restringidos. Java Card se convierte en un subconjunto del lenguaje de programación Java para aplicaciones de tarjetas inteligentes. Por tanto dispone de un subconjunto de las APIs de Java específicas para éstas y que permiten el desarrollo de *applets* Java Card como elemento central de su programación. Hereda las ventajas del uso de la tecnología de Java, permitiendo entre otras las tarjetas multiaplicación. La programación en Java Card está ampliamente aceptada y contempla la incorporación de los estándares más relevantes en los entornos de uso de tarjetas inteligentes (telefonía móvil, servicios financieros, etc.)

Las especificaciones de la tecnología Java Card, actualmente en su versión 2.2.2 (*Java Card Platform Specification 2.2.2* [SUN06]) consisten en tres partes: especificaciones de la Máquina Virtual Java Card, JCVM, que definen un subconjunto del lenguaje de programación Java y una máquina virtual para tarjetas inteligentes; especificaciones del Entorno de Ejecución Java Card, JCRE, que definen el comportamiento de las ejecuciones en tarjetas inteligentes basadas en Java; y las especificaciones de la Interfaz de Programación de Aplicaciones (API) de Java Card, que definen el núcleo y los paquetes y clases de extensiones Java para aplicaciones de tarjetas inteligentes.

La característica más significativa del entorno de ejecución de Java Card, JCRE, es que proporciona una separación clara entre el sistema de la tarjeta y las aplicaciones. El entorno de ejecución encapsula la complejidad y los detalles del sistema que se encuentra por debajo. Las aplicaciones solicitan servicios del sistema y recursos a través de una interfaz de programación de alto nivel bien definida. El JCRE es el responsable de gestionar los recursos de la tarjeta, de las comunicaciones, de la ejecución de los *applets* y de la seguridad de los procesos. Así, se compone de la Máquina Virtual Java Card, la estructura de clases de aplicación (APIs), extensiones específicas de la industria y las clases nativas del sistema.

La diferencia principal entre la máquina virtual de Java Card (JCVM) y la máquina virtual de Java es que la implementación de JCVM está dividida en dos partes: la de la máquina virtual situada en el interior de la tarjeta que incluye el *intérprete* Java Card y la parte que se encuentra fuera de ésta llamada *convertidor*.

Ambas partes componen toda la funcionalidad de una máquina virtual, es decir, la carga de ficheros de clases Java y la ejecución de los mismos. El *convertidor* carga y pre-procesa los ficheros de clases que forman un paquete Java y obtiene como resultado un fichero CAP (*Converted Applet*). El fichero CAP se carga en la tarjeta Java y se ejecuta en el *intérprete*. El *convertidor* tiene también la misión de detectar las partes del lenguaje Java no soportadas por Java Card.

Al contrario que la máquina virtual Java que procesa las clases una por una, la unidad de conversión del *convertidor* es el paquete. Los ficheros de clases se obtienen de un compilador de Java a partir del código fuente. Después, el *convertidor* preprocesa todos los ficheros de clase que forman un paquete y lo convierte en un fichero CAP. Además de este fichero CAP, el *convertidor* también genera un fichero *Export* que contiene información pública de la API para un determinado paquete e información de enlace para resolver referencias entre paquetes. El fichero *Export* no contiene código y no se carga en la tarjeta sino que el *convertidor* lo utiliza para sí mismo, realizando procesos de verificación y enlace.

Sin embargo, antes de proceder con la conversión es posible llevar a cabo un proceso de **simulación**, extremadamente útil en el desarrollo de aplicaciones para tarjetas inteligentes. En el siguiente apartado se describe brevemente el entorno seleccionado para nuestro trabajo.

Por su parte, el *intérprete* de Java Card proporciona soporte en tiempo de ejecución para el lenguaje Java y por lo tanto permite que el código de las aplicaciones sea independiente del hardware. El *intérprete* realiza las siguientes tareas: ejecuta instrucciones de código y finalmente ejecuta los *applets* (aplicaciones); gestiona la memoria y la creación de objetos; proporciona seguridad en tiempo de ejecución.

Más allá, los *applets* de Java Card no son los únicos elementos que intervienen en el conjunto de una aplicación, sino que, además de la parte de la tarjeta, se incluye la aplicación correspondiente en la parte del terminal o *host* . Ésta a su vez podría interaccionar con una aplicación remota, que conformaría el sistema. En la Figura 4.6, se muestra el esquema completo.

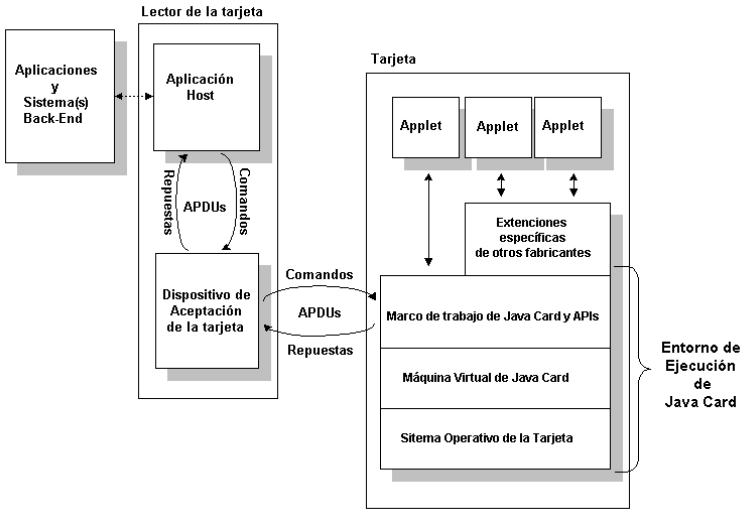

Figura 4.6 Arquitectura completa de un aplicación Java Card

Las aplicaciones *back-end* proporcionan servicios finales que sostienen las *applets* de Java en la tarjeta. La aplicación host, es la parte de la aplicación que reside en un PC, un TPV, un teléfono móvil o un subsistema de seguridad. La aplicación en el terminal

se encarga de la comunicación entre el usuario, el *applet* de Java Card, y el proveedor de la aplicación *back-end*. Tradicionalmente, las aplicaciones del lector de tarjetas se han escrito en lenguaje C. La relativa reciente expansión de la tecnología J2ME hace posible realizar la aplicación en Java en el terminal. Por ejemplo, dicha aplicación podría ejecutarse en un teléfono móvil que admite MIDP (Mobile Information Device Profile).

Uno de los modelos de comunicación entre una aplicación en el terminal y un *applet* de Java Card es el que se basa en el Paso de Mensajes (frente al modelo RMI (método de invocación remota)). En sí mismo, el modelo de paso de mensaje es la base para todas las comunicaciones de Java Card. En su núcleo está la gestión de APDUs. El marco de trabajo de Java Card recibe y envía a la comandos APDU desde/hacia el terminal (Figura 4.7) El *applet* procesa dicho comando APDU, y devuelve una respuesta en el mismo formato APDU. La comunicación entre el terminal y la tarjeta permite diferentes protocolos: orientado a byte T=0, orientado a bloque T=1; basado en USB, T=USB; o radiofrecuencia T=RF.

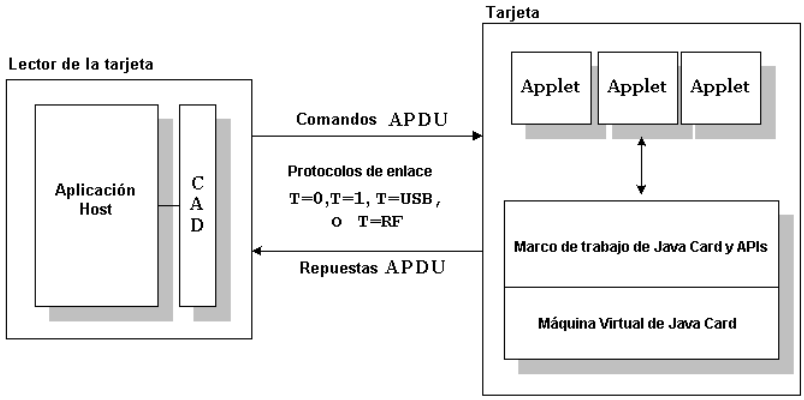

Figura 4.7 Comunicación mediante APDUs: modelo de comunicación Paso de Mensajes

4.3.2. Entorno de Simulación y Test de Sun Microsystems

Un ejemplo de simulador lo encontramos en el Kit de Desarrollo Java Card de Sun Microsystems, Java Card 2.1.2 Development Kit [JCD]. En este entorno se pueden escribir *applets* Java Card y realizar pruebas con ellos sin necesidad de una tarjeta inteligente o de un lector de tarjetas. Este kit incluye todas las herramientas básicas que se necesitan para desarrollar y probar *applets* Java Card. El simulador desempeña el papel del entorno de ejecución Java Card en un PC. En este entorno simulado, el *applet* se ejecuta en una máquina virtual Java y, por tanto, se ejecutan los ficheros .class del applet. De esta manera, el simulador puede emplear muchas de las herramientas de desarrollo Java (la máquina virtual, depuradores y otras herramientas) y nos permite probar el comportamiento del applet y ver rápidamente los resultados sin pasar por el proceso de conversión. En la Figura 4.8, se representa la arquitectura completa de este entorno de desarrollo. Los pasos indicados en la fases de compilación y test, será el objeto principal de nuestra simulación en dicho entorno.

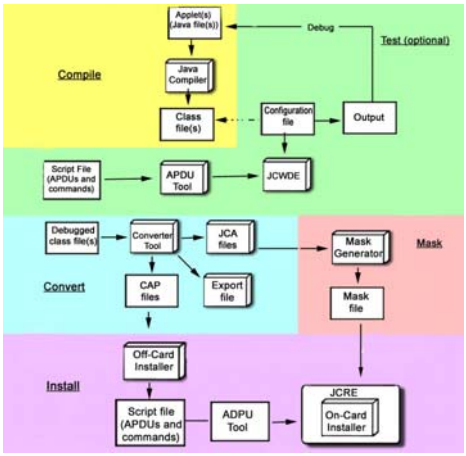

Figura 4.8 Arquitectura completa del Java Card 2.1.2 Development Kit

(Fuente: Sun Microsystems Inc.)

Las componentes de este entorno de desarrollo de las que haremos uso en la fase de simulación en nuestro trabajo se resumen en:

- Clases de la Java Card Framework, esenciales para el desarrollo de los *applets* en Java Card.

- Un entorno de desarrollo para estación de trabajo, Java Card Workstation Development Environment (JCWDE), que simula el entorno de ejecución de Java Card JCRE sobre la máquina virtual de Java, JVM.

- Herramienta APDUTool, que permite el envío de los comandos APDU al JCWDE o al JCRE.

4.4. Implementación de los Protocolos en Java Card

4.4.1. Implementación del protocolo LCP en la Tarjeta Inteligente

Para una mejor compresión de las implementaciones realizada en este punto, se presenta la estructura de las clases implementadas con Java Card en lado de la tarjeta. A continuación, se aportan los detalles sobre dichas clases.

PppEngine.class: es el *applet* central de la implementación, y tiene como objetivo principal procesar los comandos APDU recibidos y, por consiguiente, construir los comandos de respuesta. Por ello, las técnicas de mapeo descritas previamente son aquí implementadas. Como núcleo de la implementación, el trasiego bidireccional de los mensajes EAP habrán de pasar por el procesado que se lleva a cabo con este applet.

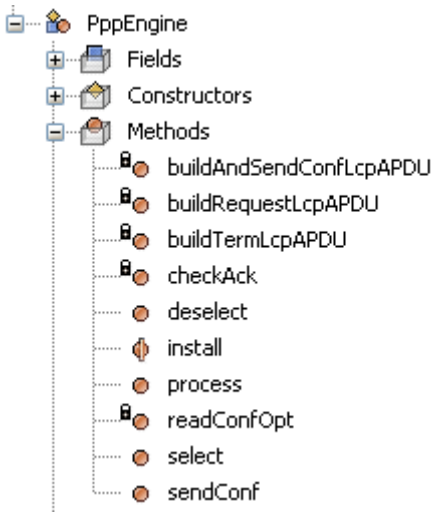

Figura 4.9 Estructura y métodos del applet PppEngine.class

PPPstate.class: es la clase encargada de llevar el control y actualización de los estados, y por tanto de su transición, del protocolo PPP. De otro, lado se ha incluido en este código el control relacionado con la secuencia de las tramas recibidas. El *applet PppEngine.class* instanciará esta clase durante el transcurso de sus operaciones.

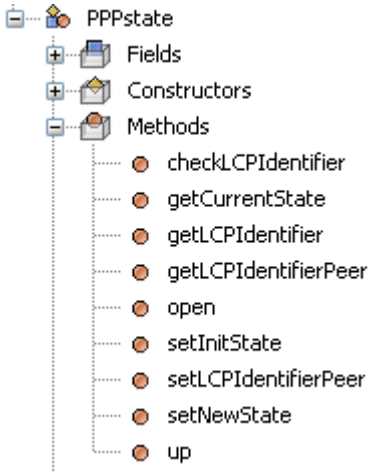

Figura 4.10 Estructura y métodos de la clase PPPstate.class

4.4.2. Implementación del protocolo EAP en la Tarjeta Inteligente.

EAPLayer.class: es una clase de Java Card que implementa las funcionalidades previstas para la capa EAP, que además de comprobar la validez de los paquetes recibidos/enviados se encarga de multiplexar/demultiplexar para entregarlos a las correspondientes capas superiores (EAPPeer/EapAuthenticator) o inferior (PPP), según Figura 4.5.

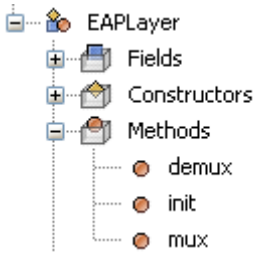

Figura 4.11 Estructura y métodos de la clase EAPLayer.class

EAPPeer.class/EapAuthenticator.class: son dos clases muy similares que tienen como principal objetivo *parsear* la petición/respuesta enviada/recibida, respectivamente, e identificar el método EAP que es aplicable en cada caso. Al mismo tiempo, estas clase son, para cada caso, las que llevan el control y actualización en la transición de la máquina de estados, incluidos en la Figura 4.5, y ahora quedan señalados en la Figura 4.12.

Figura 4.12 Estructura y métodos de la clase EAPLayer.class

EAPMethod.class: será la clase encargada de implementar el método EAP seleccionado. En principio, no es el objeto de esta implementación el de fijar método alguno, pero la implementación llevada a cabo supone una esqueleto ideal para proceder con ello. En todo caso, esta clase es respetuosa con los estándares del protocolo [Abo04] [Vol05] y en ella se aísla las funcionalidades propias de la capa EAP-Type, que hace referencia al tipo de método de autenticación soportado (Figura 4.13).

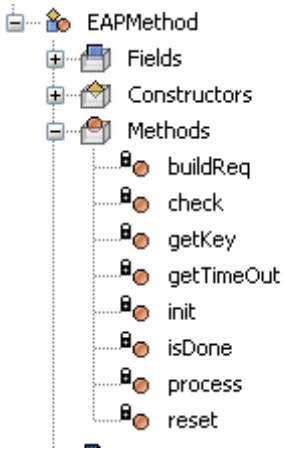

Figura 4.13 Estructura y métodos de la clase EAPMethod.class

4.4.3. Implementación en el Terminal

La implementación en el Terminal ha sido orientada netamente a la posterior evalución de funcionalidades prevista en esta tesis. Por tanto, responde únicamente al interfaz que comparte con la tarjeta inteligente.

En primera instancia y con respecto al primero de ellos se ha hecho uso de la herramientas APDUTool y JCWDE en la fase de test. El objetivo de iniciar la implementación con esta herramienta ha sido el de poder establecer toda una metodología de pruebas basadas en tests específicos con casos de uso, que ponen a prueba la implementación realizada en la tarjeta y la factibilidad de los modelos definidos en este trabajo. Esta herramienta permite lanzar un conjunto de *scripts* que en sí mismo constituyen una secuencia comandos APDU en los que el mapeo de los protocolos LCP y EAP se han realizado según las técnicas descritas. La migración desde este entorno de pruebas basadas en scripts hacia una sencilla aplicación en Java que realice esta funcionalidad a partir de tramas reales EAP, permanece que trabajo futuro de esta tesis. Para entender mejor la implementación a realizada en el terminal, emplazamos al lector al siguiente capítulo, donde se describe extensamente ésta para la realización de las pruebas y evaluación.

4.4.4. Conclusiones sobre la Implementación

Con la realización de la fase de implementación, los modelos sobre los que se ha trabajado en esta tesis han tomado relevancia como proceso de acercamiento desde la visión conceptual del problema hacia el plano de su aplicación. A pesar de las pruebas preliminares de realizadas de este diseño, durante el proceso de implementación aquí descrito, en este punto, se hace necesario un riguroso proceso de evaluación de la misma, de la que daremos cuenta en el próximo capítulo. Según el resultado de dicha evaluación, estaremos en disposición de valorar la viabilidad de la aplicación del Marco

de Autenticación para Tarejtas Inteligentes en Red que soporta esta implementación, a un escenario concreto.

Capítulo 5.

Evaluación de Funcionalidades y Análisis de Resultados

5. Evaluación de Funcionalidades y Análisis de Resultados

5.1. Diseño de la Evaluación de Funcionalidades para Tarjetas Inteligentes

En este capítulo se llevan cabo los tests que suponen la evaluación de funcionalidades incluidas en los modelos propuestos en esta tesis e implementados según se describe en el capítulo anterior. El foco principal de los mismos apunta hacia el Modelo de Multiplexación EAP para tarjetas inteligentes descrito en el apartado 3.6.2 y representado en Figura 3.16. El objeto este enfoque se basa en el hecho que una adecuada implementación de dicho modelo, corroborado por la oportuna evaluación, apuntaría hacia la viabilidad del Modelo Extendido de Autenticación y en concreto hacia la Arquitectura de Protocolos de Autenticación para tarjetas inteligentes descritos en el capítulo 3 de este documento. Por tanto, en esta fase se diseñan y desarrollan un conjunto de pruebas que permitirán demostrar la factibilidad de los planteamientos asentados en la presente tesis.

Como quedó introducido en el capítulo anterior, como entorno de trabajo se ha elegido el simulador disponible en el Kit de Desarrollo Java Card de Sun Microsystems, Java Card 2.1.2 Development Kit [JCD]. Este kit incluye todas las herramientas básicas que se necesitan para desarrollar y probar *applets* Java Card. El simulador interpreta el papel del entorno de ejecución Java Card en un PC. De esta manera, el simulador puede emplear muchas de las herramientas de desarrollo Java (p.e. depuradores y otras herramientas) y nos permite probar el comportamiento del applet. En la Figura 5.1, se representa la arquitectura parcial del simulador en este entorno de desarrollo, de la que destacamos los elementos que componen nuestro Banco de Pruebas.

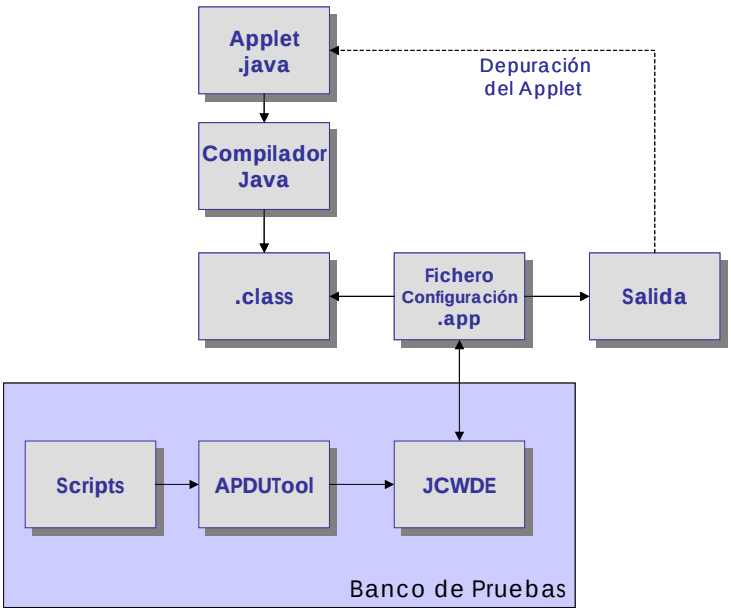

Figura 5.1 Simulador y Banco de Pruebas

Scripts. Es un lenguaje codificado específico para este entorno aunque bastante similar otros. El comienzo de cada script se identifica por la sentencia `powerup;`. De la misma forma la finalización se especifica mediante la sentencia `powerdown;`. Ambas emulan los comandos de inicializan y finalización de la comunicación entre la tarjeta inteligente y el terminal. Entre ambas sentencias se incluyen el conjunto de comandos APDU que se desea transmitir a la tarjeta y de los que se ha de esperar la respuesta en función del procesamiento que la tarjeta emulado de cada uno de esos comandos en función de lo especificado en el applet que debe procesar dichos comandos. Para ello, el fichero de script debe comenzar con ciertos comandos APDUs encargados de instanciar un primer applet genérico denominado Instalador. A continuación el script debe incluir un comando APDU para reservar recursos (registro) para el *applet* a seleccionar , que es sí mismo la aplicación objetivo *PppEngine.class* descrita en el apartado 4.4.1. En la Figura 5.2 se representa los pasos de ejecución de un *script* genérico.

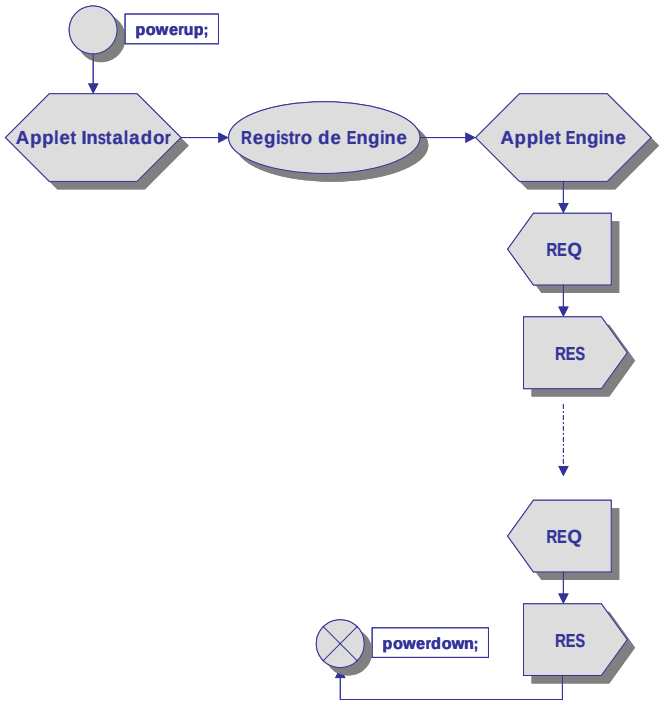

Figura 5.2 Pasos de Ejecución de un Script Genérico

El aspecto que toman estos comandos APDUs en un fichero de script se representa en la Figura 5.3.

```
//+
// Workfile:@(#)eap.scr   0
// Version:1.10
// Date:02/25/06
//-

powerup;

// Selecciona el Applet Instalador
0x00 0xA4 0x04 0x00 0x09 0xa0 0x00 0x00 0x00 0x62 0x03 0x01 0x08 0x01 0x7F;
// 90 00 = SW_NO_ERROR

echo "Seleccionado el Applet Instalador";

// Registro PPPengine,java
0x80 0xB8 0x00 0x0 0x0d 0x0a 0xa0 0x0 0x0 0x0 0x62 0x3 0x1 0xc 0x1 0x1 0x01 0x00 0x7F;

echo "Registradp el Applet PppEngine.java";

// selecciona Applet PppEngine.java
0x00 0xA4 0x04 0x00 0x0a 0xa0 0x0 0x0 0x0 0x62 0x3 0x1 0xc 0x1 0x1 0x7F;

echo "Seleccionado el Applet PppEngine";


// Envío de paquete CONF_REQ
0xA4 0x01 0x41 0x0C 0x08 0x03 0x04 0xC2 0x27 0x01 0x04 0x01 0x00 0x7F;

echo "Evento: RCR+.Debe devolver un ACK";

// Envío de paquete EAP_REQ
0xA0 0x01 0x01 0x08 0x04 0x01 0x04 0x04 0x4 0x7F;

echo "Evento: EAP-REQ-ID";

powerdown;
```

Figura 5.3 Script simplificado ejemplo

Para un adecuado proceso de depuración de la implementación de los protocolos, cada uno de los comandos APDU (trama LCP o EAP) ha ido acompañado de un segundo comando, definido *ad hoc*, para probar en cada momento el estado del *automaton* de los mismos, como evaluación de las funcionalidades implementadas. En la Figura 5.4 se representa los pasos de ejecución propios de un script en los que se han incluido los comandos APDUs de Chequeo del Estado del Protocolo CEP_LCP o CEP_EAP, simbolizando con EP_LCP o EP_EAP, el Estado del Protocolo en cada momento. Obviamente, esta monitorización en el banco de pruebas ralentizará el proceso pero se hace imprescindible en durante esta fase.

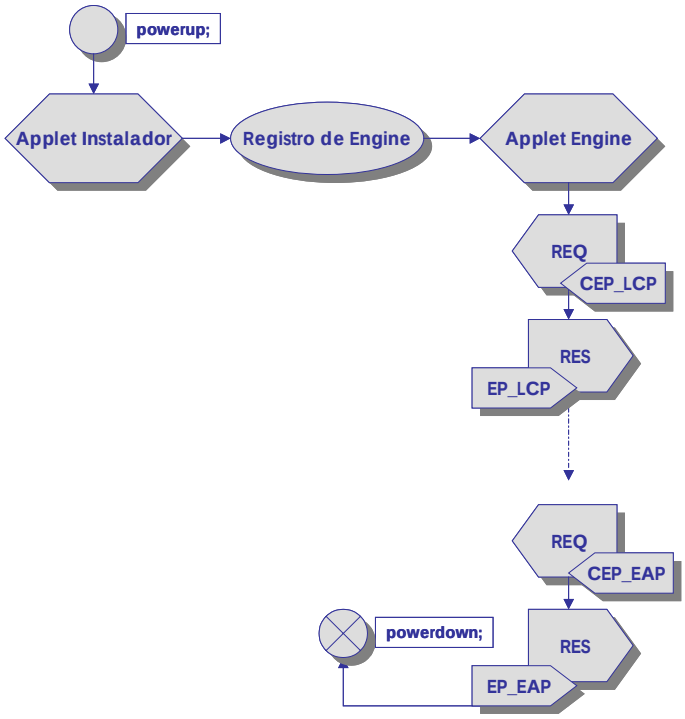

Figura 5.4 Pasos de Ejecución de un Script en el Banco de Pruebas

Como metodología en la evaluación de funcionalidades, se realizan inicialmente tests independientes por cada uno de los protocolos, chequeando en cada caso que responden adecuadamente a su *automaton*. En los siguientes apartados se detallan dichos tests.

5.1.1. Evaluación de Funcionalidades de LCP en Tarjeta Inteligente

Los tests desarrollados, como evaluación de funcionalidades, se realizan mediante un fichero *script* para cada caso, basados en el esquema representado en la Figura 5.4. Los siguientes scripts y se han desarrollado a lo largo de este trabajo, valorándose el resultado de cada uno en Tabla 5.1.

Script	Descripción	Resultado
configReqAck.scr	Configuración correcta del enlace LCP. Se activa Capa EAP	√
configReqNack1.scr	Configuración incorrecta del enlace LCP. No se activa Capa EAP	√
configReqNack2.scr	Identificador duplicado en la trama LCP. No se activa Capa EAP	√
configReqRej.scr	Trama LCP defectuosa. No se activa Capa EAP	√
configTermReqAck.scr	Configuración correcta del enlace LCP. Se activa Capa EAP. Finalización correcta del enlace. Se desactiva Capa EAP.	√

Tabla 5.1 Scripts para la evaluación de la implementación de LCP para tarjetas inteligentes

Como resultado de los tests realizados en este apartado se comprueba la correcta implementación de la máquina de estados simplificada y prevista en nuestro trabajo (Tabla 4.2), para la fase de establecimiento del enlace del protocolo PPP.

5.1.2. Evaluación de Funcionalidades de EAP en Tarjeta Inteligente

La correcta implementación del protocolo LCP, nos permite probar a continuación el comportamiento del protocolo PPP en la fase de autenticación. Para ello, los scripts desarrollados en este apartado deben incluir el script *configReqAck.scr* que facilita el adecuado establecimiento y configuración del enlace, incluyendo la activación de la capa EAP (*EAP Layer*), según nuestro Modelo de Multiplexación EAP para tarjetas inteligente.

De forma análoga a como se ha realizado para el caso de LCP, los siguientes scripts se han desarrollado para la evaluación del Modelo de Multiplexación EAP para tarjetas inteligentes, valorándose el resultado de cada uno en Tabla 5.2.

Script	Descripción	Resultado
ReqIdent.scr	Solicita Identidad. Multiplexa a Capa Peer.	√
ReqIdent2.scr	Solicita Identidad. Multiplexa a Capa Peer. Activa Capa Method. Responde Identidad	√
success.scr	Solicita Identidad. Multiplexa a Capa Peer. Activa Capa Method. Responde Identidad. Comprueba Identidad y OK	√
failure.scr	Solicita Identidad. Multiplexa a Capa Peer. Activa Capa Method. Responde Identidad. Comprueba Identidad y NOK	√
notification.scr	Envía notificación. Multiplexa a Capa Peer. Activa Capa Method.	√

Tabla 5.2 Scripts para la evaluación de la implementación del Modelo de Multiplexación EAP para tarjetas inteligentes

5.2. Análisis de Resultados

5.2.1. Evaluación del ajuste al modelo

A la vista de los resultados obtenidos en la realización de los tests descritos en el apartado anterior, podemos añadir que tanto por la metodología de diseño como las posibilidades ofrecidas por Java Card, ha sido posible un correcto ajuste al Modelo de Multiplexación EAP para tarjetas inteligentes, propuesto en nuestro trabajo, dada las pruebas y resultados obtenidos en entorno de simulación. Estos resultados nos permiten incluirlos como parte del Modelo Extendido de Autenticación, lo que habrá de derivar

en la implementación de la Arquitectura de Protocolos de Autenticación (Figura 3.17), bajo la garantía del cumplimiento de los estándares oportunos.

5.2.2. Viabilidad de aplicación

Estos resultados nos permiten afrontar su aplicación en un escenario potencial. Con el objeto de contribuir en términos de practicidad y aplicabilidad con la elaboración de esta tesis, se procederá en el próximo capítulo a la aplicación del nuevo Marco de Autenticación, con el objeto de considerar su viabilidad en un escenario concreto. El escenario de interés, y al que se le ha dedicado un importante espacio en el transcurso de nuestra investigación, sería el del pago electrónico con una tarjeta inteligente *auto-autenticable.*

Capítulo 6.

Aplicación a escenarios de Pago Electrónico en entornos Inalámbricos

6. Aplicación a escenarios de Pago Electrónico en entornos Inalámbricos

El objetivo principal de este capítulo es el de confrontar el *Marco de Autenticación para Tarjetas Inteligentes en Red* desarrollado en esta tesis, con un escenario potencial, en aras de explorar su aplicabilidad y utilidad, en términos prácticos.

Durante la elaboración de nuestro trabajo, han sido necesarios un conjunto de estudios que nos ha obligado a profundizar en las tecnologías involucradas en los procesos de autenticación junto con la tarjeta inteligente y en la evolución que en dichas tecnologías se han producido. Para acometer este capítulo de aplicación ha sido necesario identificar, no sólo un escenario actual en el que tuviera cabida de forma aplicada nuestro Marco de Autenticación, sino también las tendencias que podrían apuntar hacia escenarios venideros. Si bien en los antecedentes de este trabajo, de los que se dio cuenta en el capítulo 2, se ha dejado constancia del tipos potenciales de redes de acceso e infraestructura al que enfrentarán las tarjetas inteligentes de nueva generación, en el presente capítulo se abordan los aspectos referidos a los terminales de acceso y a los servicios de autenticación en un contexto determinado. El conjunto deberá conformar un escenario realista sobre el que cabrá la aplicación del Marco de Autenticación aquí elaborado.

En concreto, el escenario seleccionado es el del *Pago Electrónico* según los términos en los que se discutió en la introducción de este documento. Por tanto, la mutua autenticación remota de la tarjeta inteligente *presencial* de crédito/débito como medio de pago, será objeto de estudio en los próximos epígrafes. Las tecnologías y servicios particulares que forman parte de dicho escenario quedan ampliamente justificados por la representatividad e implantación masiva a medio/largo plazo, y que podrían caracterizarlo según los estudios de tendencias que se aportan.

El segundo objetivo que se persigue en el presente capítulo, es el de demostrar las ventajas que el Marco de Autenticación aplicado presenta, en tanto que facilita la migración *suave* de los mecanismos de autenticación previstos en las especificaciones para las tarjetas inteligentes actuales hacia los de una futura generación, en un escenario concreto como el que aquí se propone.

En los próximos apartado, se tratan pormenorizadamente los procesos de evolución por los que se ven afectados los terminales que dan acceso al sistema transaccional, de un lado, y las tarjetas inteligentes en aplicaciones bancarias, por otro.

6.1. Terminales Punto de Venta y Redes Inalámbricas

El estudio de la evolución de los dispositivos denominados Terminales de Punto de Venta, TPV (POS), nos lleva al primero de los casos de evolución tecnológica a considerar.

Históricamente, estos terminales –también conocidos como datáfonos-, conectados directa o indirectamente al correspondiente banco por línea telefónica fija, han permitido y permiten solicitar la autenticación y autorización de un pago desde su ubicación (restaurantes, comercios, etc.). Con la llegada de las tarjetas inteligentes, estos terminales han debido sustituir el lector de banda magnética por el adecuado para aquellas. Más allá, han incorporado también el software oportuno para el intercambio de mensajes de autenticación tanto con dichas tarjetas como con el sistema bancario; todo ello, según la normativa de homologación que, normalmente, las entidades de servicio financiero han dictaminado.

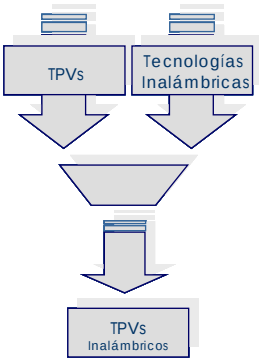

Figura 6.1 Evolución tecnológica hacia los TPVs inalámbricos

La evolución relativa a estos dispositivos, Figura 6.1 tiene que ver con la incorporación masiva en el mercado en los últimos años de tecnologías inalámbricas, dando lugar a los consecuentes TPVs inalámbricos (wireless POS o wPOS). En primera instancia, estos dispositivos hacían uso de redes de telefonía móvil (GPRS/UMTS) para establecer comunicación con el banco emisor o la entidad financiera correspondiente, con el objeto de autenticar la tarjeta y autorizar el pago electrónico [LIPMAN][THALES]. En este caso, los mensajes relativos al pago viajan en todo momento a lo largo de la red bajo el dominio administrativo del operador de telefonía móvil, garantizando en todo momento éste la salvaguarda de dicha información durante su tránsito.

Si bien es cierto que no es común el transporte de esta información sensible a través de redes públicas como Internet, esto no impediría que la red de acceso el TPV sin cable pudiera ser una red de área local (inalámbrica) en el punto de venta, siempre y cuando las medidas de seguridad adoptadas y el ejercicio de responsabilidad del operador correspondiente se establecieran en sus máximos niveles. Esta tendencia en el acceso multimodo parece estar consolidada tecnológicamente dada la multitud de productos que se encuentran disponibles.

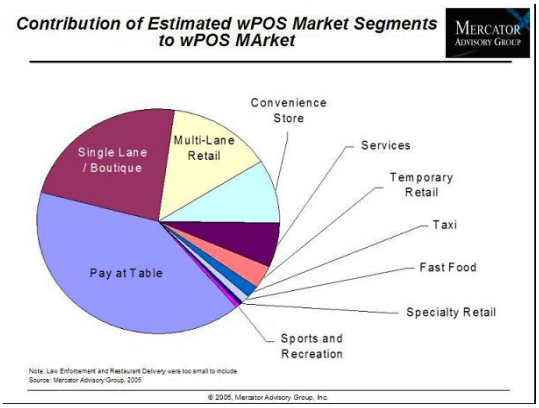

Figura 6.2 Contribución de los TPVs inalámbricos por sectores en 2005

(Fuente: Mercator Advisory Group)

Estudios recientes y solventes (Figura 6.2) auguran una relevante penetración en el mercado de estos TPVs inalámbricos, siendo los sectores de la restauración y comercios principales agentes de demanda. Ajenos a un proceso de estandarización específico, la implantación en el mercado de estos dispositivos depende de la homologación pertinente y, más allá, de los intereses en las directrices de negocio de entidades bancarias y de servicios financieros.

Tal como se introdujo y justificó en el Capítulo 1 de este documento, parece razonable considerar que la red a la que accederán los TPVs sin cable, y por ende las tarjetas inteligentes de nueva generación, sea una red inalámbrica de interconexión, PWLAN. Con este último apunte podríamos caracterizar aún más nuestro escenario de aplicabilidad como: *pago electrónico en entornos inalámbricos.*

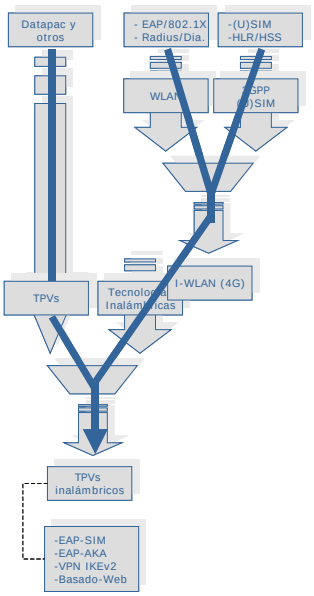

Figura 6.3 Convergencia de los mecanismos de autenticación para TPVs inalámbricos

Referido a la consecuente convergencia que se produce en el plano de la autenticación, Figura 6.3, se ha de considerar que los TPVs tradicionales además de comunicarse con tecnologías cableadas hacen de uso de estándares específicos [ISO 8583-1] y en muchos casos propietarios (Visa-BaseII), de entornos financieros y bancarios. Con el proceso convergencia que los conecta a la red de forma inalámbrica y con la proliferación de otras tecnologías de acceso y de red, esta evolución, en nuestra opinión, apunta hacia unos protocolos y mecanismos de autenticación resultantes basados en la existencia de un módulo (U)SIM tanto para el caso en el que la red inalámbrica sea exclusivamente del tipo 3GPP o de interconexión PWLAN. Esto podría traducirse en una migración *suave* cada vez más consolidada hacia soluciones basadas en EAP-SIM [Hav06], EAP-AKA [Ark06], etc. de fácil implementación en dichos TPVs inalámbricos.

6.2. Tarjetas bancarias y tarjetas inteligentes

Aun cuando la patente de tarjetas inteligentes registrada por Roland Moreno en 1974 y las primeras estuvieran disponibles a finales de esa década, no fue hasta el periodo 1982 –84 cuando los bancos franceses realizaron experimentos con el objeto de evaluar la viabilidad económica y la factibilidad técnica de tres tipos de tarjetas inteligentes de distintos fabricantes. Es probablemente en este punto donde comienza la convergencia entre las tarjetas de banco tradicionales, de tecnología de banda magnética, y las modernas tarjetas inteligentes. Como resultado de estos experimentos, los bancos eligieron las tarjetas con procesador Bull CP8, que se generalizaron en toda Francia a partir de 1986.

Las tarjetas inteligentes proporcionaban un medio ideal para dotar de seguridad ciertas operaciones bancarias. Podían almacenar claves secretas de forma segura y también ejecutar algoritmos criptográficos. Adicionalmente, su facilidad de manejo, el tamaño reducido, la continuidad en la forma respecto a las tarjetas conocidas y el hecho de que pudieran ser empleadas en casi cualquier parte por el usuario, fueron factores que animaron a los bancos y entidades de servicios financieros a desarrollar aplicaciones y tecnologías seguras basados en estos dispositivos.

En esta línea, entidades de servicios financieros vienen propiciando la migración definitiva de las tarjetas tradicionales de crédito hacia las tarjetas con chip. La necesidad de un proceso de especificaciones que soporte la estandarización de las tarjetas inteligentes para fines bancarios o financieros culmina con la elaboración de los libros de EMV –ya referenciados–, y que justifican, dada la relevancia de las entidades que la respalda, la tendencia de la que pretendemos dar cuenta en esta tesis, Figura 6.4.

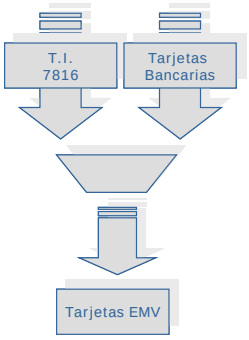

Figura 6.4 Evolución tecnológica hacia las Tarjetas Inteligentes EMV

En la Tabla 6.1 se muestran algunos datos recientes de la implantación de las tarjetas EMV en Alemania, Francia y España.

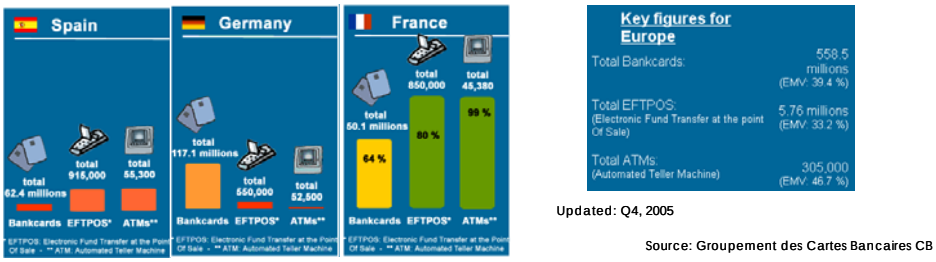

Tabla 6.1 Datos de la implantación de las especificaciones EMV en Europa

La Figura 6.5 ilustra la clara tendencia en la implementación de esta especificación para el pago electrónico con las tarjetas inteligentes.

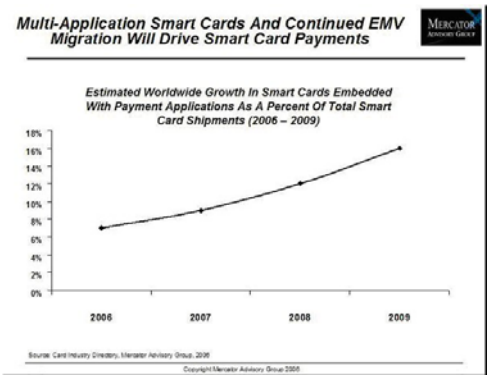

Figura 6.5 Tendencia de la migración a aplicaciones EMV integradas en las tarjetas inteligentes de pago (Fuente: Mercator Advisory Group)

En cuanto a la convergencia producida en el ámbito de los protocolos y mecanismos de autenticación a la que este proceso obliga, se parte de técnicas y algoritmos de criptografía tanto simétrica como asimétrica, que las tarjetas inteligentes pueden ofrecer cada vez más eficientemente; hecho que aprovechan las entidades de servicios financieros para promover el desarrollo de tecnología y aplicaciones en entornos bancarios, con el objetivo de fortalecer los procesos de autenticación más tradicionales, por ejemplo, los basados en PIN (on-line u off-line). Como resultado, aparecen las especificaciones EMV, y en concreto el libro 2, se dedica íntegramente a la seguridad en las transacciones con este tipo de tarjetas y muy especialmente en los procedimientos de autenticación (*Book 2: Security and Key Management*) [EMV04-2]. En estas especificaciones quedan previstos cuatro tipos distintos de autenticación. Tres de ellas se realizan con criptografía asimétrica y siempre en situaciones en las que no existe conectividad con la entidad emisora de tarjetas (off-line), por tanto en un enfuqe claramente distribuido; y una cuarta opción para cuando sí está prevista la conectividad con dicha entidad (on-line), en cuyo caso se procede con mecanismos de autenticación basadas en criptografía simétrica. De la relevancia para nuestra tesis de este último procedimiento de autenticación, quedará constancia a lo largo del presente capítulo.

Pero más allá, entendemos que las inercias detectadas habrá de llevarnos a contemplar un proceso gracias al cual la tecnología desplegada al efecto debería permitir una harmonización, en la manera que las tarjetas EMV y sus procedimientos de autenticación fueran acordes con las tendencias marcadas para la NGTI. En este sentido, es significativamente interesante para nuestro trabajo, todo lo relativo al esquema de autenticación remota (on-line) ya que podría ser tratado bajo nuestro enfoque basado en infraestructura. En definitiva, la contemplación de esta tendencia hacia las tarjetas inteligentes conectadas a la red, en la implantación de estas especificaciones, se hace imprescindible junto con el resto de los elementos que habrán de componer el esquema de pago electrónico. El conjunto acota el plano de aplicación en el que pretende poner el acento esta tesis.

Sin embargo en nuestra opinión, el proceso que debería permitir la migración suave de los protocolos y mecanismos de autenticación on-line definidos para las tarjetas EMV hacia las emergentes tarjetas de la NGTI, no sólo no está resuelto sino que requiere del correspondiente estudio, Figura 6.6. Así, las especificaciones EMV se limitan a determinar un protocolo de autenticación remota genérico para tarjetas inteligentes en pago electrónico, cuyo diseño, aunque tiene soporte remoto, está enfocado al medio de acceso respecto a la tarjeta, tal como se explicó en el análisis realizado en el capítulo 3; esto indica que dichas especificaciones no atienden en ningún momento a la infraestructura en el esquema de autenticación remota, y podría no ser lo suficientemente robusto o interoperable como para permitir una migración de bajo impacto hacia tecnologías de red, tal como se prevé en la NGTI.

Buena muestra de ello, puede observarse en la falta de atomicidad del diseño de los protocolos y mecanismos de autenticación, que en EMV siguen descansando en buena medida en el terminal, y comportándose ambos tarjeta-terminal, como un solicitante de autenticación dividido y en ningún caso con la autonomía requerida por parte de una tarjeta inteligente, que participa en un pretendido proceso de seguridad, como es el caso del pago electrónico. Más detalles sobre estos aspectos pueden encontrarse en próximas secciones de este capítulo.

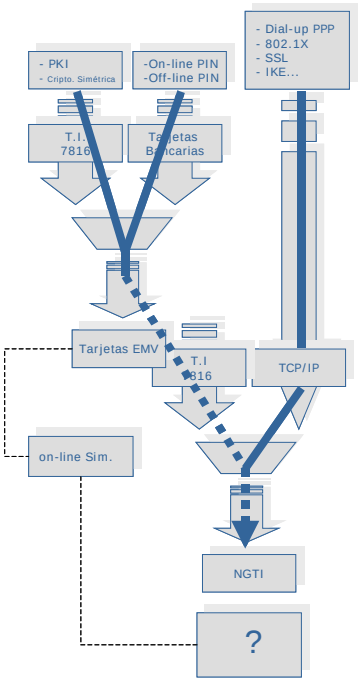

Figura 6.6 Convergencia de los protocolos de autenticación EMV en las tarjetas NGTI

A modo consideración final en este epígrafe, podemos concluir diciendo que el conjunto de convergencias tecnológicas detectadas en esta tesis podrían estar implicadas como componentes de escenarios emergentes de pago electrónico con tarjetas inteligentes, representando un impacto indudable no sólo en los protocolos de autenticación en cada una de ellas, sino también en el esquema global que los relacionan, Figura 6.7. De este punto se deriva la problemática de armonizar los protocolos y mecanismos de autenticación desde una perspectiva común; desde un Marco de Referencia único que contemple todos los componentes del procedimiento de autenticación al unísono. Nuestro Marco de Autenticación para Tarjetas Inteligentes en Red atiende a este enfoque del problema.

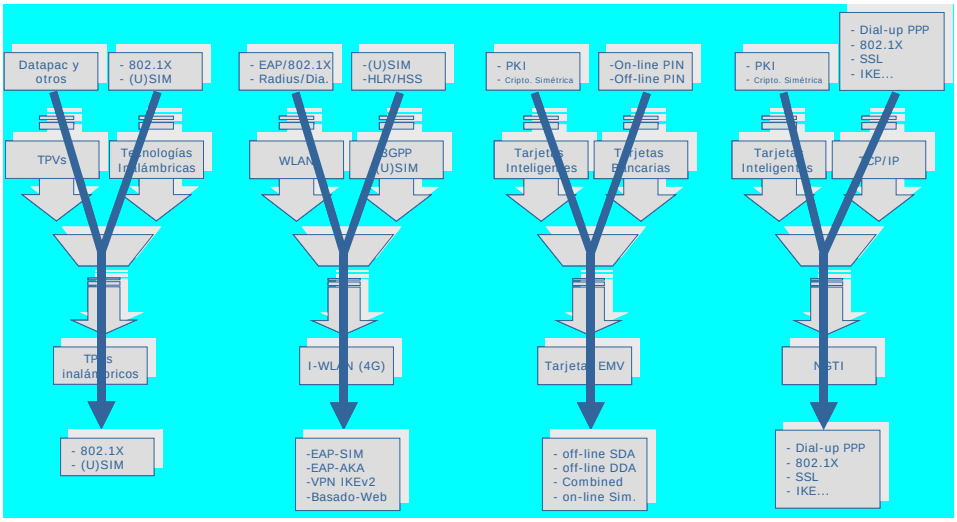

Figura 6.7 Convergencia tecnológica para escenarios de pago electrónico en entornos inalámbricos

6.3. Descripción del escenario de Pago Electrónico en entornos Inalámbricos

El escenario de interés y objeto de aplicación, queda ilustrado en la Figura 6.8. Se trata de un escenario de pago electrónico con tarjeta inteligente a través de una infraestructura de interconexión de redes inalámbricas, PWLAN. En él, una tarjeta inteligente es caracterizada como una tarjeta de crédito/débito, asumiendo la presencia de un usuario en un pago con tarjeta bancaria presencial, actuando ésta última en el rol del dispositivo solicitante, DS. De otro lado, el WLAN-EU podría tratarse de un Terminal Punto de Venta inalámbrico, TPVi (*Wireless Point of Sale, WPOS*) ubicado en las dependencias de un comercio físico y que estaría caracterizado como un dispositivo móvil provisto de un módulo (U)SIM y por tanto registrado en un HLR/HSS perteneciente a una red de tercera generación gestionada por un operador de telefonía móvil. En este contexto, el servidor 3GPP AAA (p.e. servidor RADIUS) podría estar bajo el control directo o indirecto del Emisor de la tarjeta (banco o entidad de servios financieros), o por un Procesador de Pagos actuando en su nombre, en tanto que es la entidad responsable de autenticar el TPVi y a la tarjeta inteligente, según las especificaciones EMV. El modelo de negocio derivado de los acuerdos necesarios entre las partes involucradas (operador de telefonía móvil y bancos) podría recaer en el estudio futuro pendiente en este trabajo. Cabe decir que una aproximación a un escenario similar fue considerada por el autor en [Tor05].

En el caso particular de una situación de *roaming*, tal como se muestra Figura 6.8, la petición/ respuesta de autenticación es redirigida desde el servidor AAA, que en tal caso actuaría como servidor de autenticación intermediario (3GPP proxy AAA) en la red de telefonía visitada, hacia tal servidor en nuestra red de telefonía, cuyo operador nos reconoce como abonado, y viceversa. Siendo en estas circunstancias igualmente válido el Modelo Extendido de Autenticación propuesto en nuestro trabajo (epígrafe 3.2).

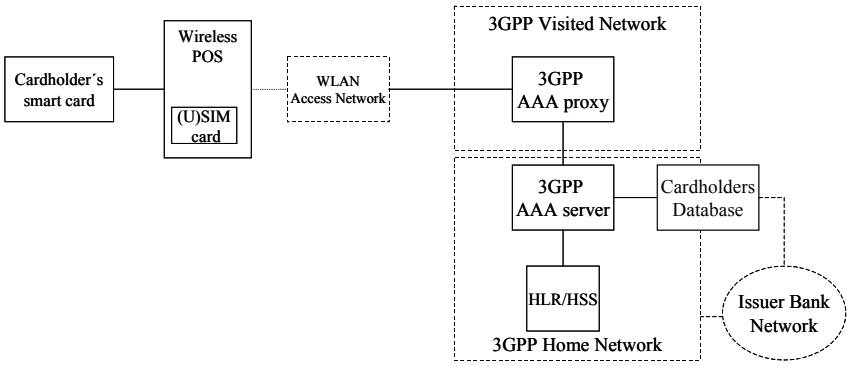

Figura 6.8. Escenario de aplicación: Pago Electrónico con Tarjetas Inteligentes, en entornos Inalámbricos

Los puntos de acceso, PAs, de la red local inalámbrica, así como los posibles *proxies* a través de otras redes, deberían permanecer *transparentes* en el proceso de autenticación mutua extremo-a-extremo. Sin embargo, la necesidad de una tarjeta inteligente (en el rol de nSA) para el pago en este escenario realista introduce cierta complejidad que ya ha sido estudiada en este trabajo. Así, por razones de seguridad y basándonos en nuestro Modelo Extendido de Autenticación, nuestra propuesta propone que el TPVi realice funciones de autenticador (nAUT) en este proceso, minimizando los riesgos de ataques potenciales desde un TPVi no confiable y haciendo más robusto el proceso de autenticación mutua en el que participa dicha tarjeta. En este caso, un servidor 3GPP AAA (SAUT) es el encargado de autenticar la tarjeta inteligente tomando como referencia los registros realizados en la oportuna base de datos. Una vez más, dependiendo de los acuerdos entre el Emisor y los operadores de telefonía móvil dicho servidor y las bases de datos asociadas podrían estar integrados en los dominios administrativos de unos u otros.

El proceso de pago en este escenario podría resumirse de la siguiente manera. Una vez que el TPVi es autenticado por el Emisor actuando en su nombre (en ciertos casos, esta tarea se podría realizar con la cooperación de un banco adquiriente; ambas circunstancias quedan al margen de nuestro trabajo), según el Modelo Genérico de Autenticación (Figura 3.7a), entonces se procede con la aceptación de la tarjeta de pago en dicho Terminal Punto de Venta. Como se ha mencionado, en nuestro modelo la tarjeta inteligente incorpora de forma completa la funcionalidad de solicitante de autenticación (rol de *Supplicant*), evitando la versión de solicitante dividido (*split-supplicant*) empleada hasta el momento. Así, con el objeto de formalizar un pago, la tarjeta de pago podría ser autenticada en primera instancia por el Emisor, e idealmente viceversa, y de forma independiente al proceso de autenticación llevado a cabo por el usuario, mediante sus propios credenciales contra el Emisor, y al llevado a cabo por el TPVi.

Por tanto, las funciones previstas para la tarjeta inteligente deberían ser:

- intercambio de mensajes con el servidor AAA con el objeto de completar un proceso de autenticación autónomo con el Emisor, y que debe contemplar el almacén seguro de los credenciales oportunos de la propia tarjeta,
- ejecutar una aplicación de pago electrónico seguro,
- comunicarse con la aplicación que corre en el lado del TPVi (normalmente denominado *Cardholder Client System software*),
- generar y devolver los criptogramas de acuerdo al método de autenticación,
- almacenamiento de otros credenciales del usuario de forma independiente,
- implementar el Modelo de Multiplexación EAP dentro de la Arquitectura de Protocolos de Autenticación, para tarjetas inteligentes, propuesto en esta tesis.

Por su parte, las funcionalidades previstas para el TPVi en este escenario son:

- asociación a una infraestructura de interconexión de redes 3G/WLAN, según el Modelo Genérico de Autenticación,

- portador y servidor para el acceso de la tarjeta inteligente al resto del sistema, en el rol de autenticador (nAUT). Esta última funcionalidad viene derivada de nuestro Modelo Extendido de Autenticación,
- ejecutar una aplicación de pago electrónico seguro y almacenar sus propias credenciales de seguridad,
- reenvío de mensajes de autenticación entre la tarjeta inteligente y su Emisor,
- implementación acorde a la Arquitectura de Protocolos de Autenticación, para WLAN-EU, propuesta en esta tesis.

Es importante recordar en este punto, que los servicios de interés en este escenario son sólo aquellos referidos exclusivamente a los procesos de autenticación, excluyendo así todos los mecanismos y técnicas que tienen que ver con la provisión de servicios de tipo IP, a los que se accedería en los escenarios que tuvieran cabida, una vez superada la fase de autenticación. Otras aplicaciones o servicios descansan en el objeto de trabajos futuros.

6.4. Especificaciones para Transacciones de Pago Electrónico con Tarjetas Inteligentes, EMV

Las especificaciones EMV [EMV], ya introducidas en el Capítulo 1, contemplan distintos esquemas de autenticación de tarjetas inteligentes en el contexto de los pagos electrónicos. Según se ha explicado en este capítulo, dichas especificaciones determinarán, en gran medida, el futuro de las actuales tarjetas de pago electrónico y por tanto resulta de especial interés su consideración como aplicación de nuestro Marco de Autenticación. Conviene reseñar el hecho de que la utilización de dichas tarjetas en estos escenarios, así como en los de comercio electrónico/ móvil, queda reflejada también en los estándares y recomendaciones más relevantes [3DS01]. Si bien todos ellos consideran la posibilidad de que estas tarjetas fueran insertadas en dispositivos inalámbricos/ móviles, no contemplan dentro de su alcance la tecnología de red que subyace; o dicho de otro modo, la infraestructura formada por las tecnologías de red de acceso o la interconexión de redes.

En las próximas secciones se hace una detallada descripción de estas especificaciones, incidiendo básicamente en los puntos que pueden incluirse bajo el alcance de esta tesis.

6.4.1. Flujo de una Transacción en EMV

Para una mejor comprensión de los procesos de autenticación definidos en EMV, y en concreto del caso particular que tomaremos para una posterior implementación, se hace necesaria una introducción a los pasos que tienen lugar en el proceso de una transacción de compra con tarjetas inteligentes en escenarios de pago electrónico, en la que el procedimiento de autenticación está íntimamente presente. En los próximos apartados se detallarán aspectos propios de las distintas opciones de autenticación existentes.

En todo momento será la tarjeta la que limitará las posibilidades en función de su configuración y que queda recogida en su Perfil de Intercambio de Aplicación (*Application Interchange Profile*, AIP), por tanto el TPVi, en adelante Terminal, sólo deberá intentar ejecutar aquellas funciones que la tarjeta soporta. El diagrama de flujo ilustrado en la Figura 6.9 se detalla cada una de las funciones de una transacción, incluyendo aquellas que podrían ser opcionales, y que en los próximos apartados pasamos a describir brevemente.

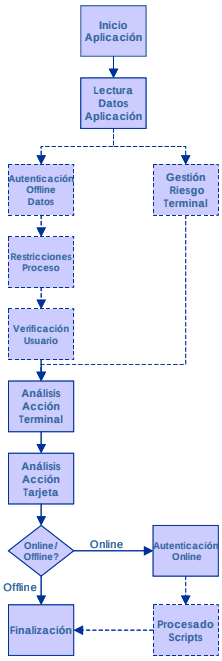

Figura 6.9 Flujo de una transacción según EMV

6.4.1.1. Procesamiento del Inicio de la Aplicación (comando GET PROCESSING OPTIONS)

El Terminal realizará las siguientes tareas, justo tras la consecución de la selección de la aplicación (comando SELECT):

- informa a la tarjeta que una nueva transacción se va a realizar,
- proporciona a la tarjeta la información relativa a dicho Terminal para esa transacción,
- obtiene de la tarjeta el AIP y una lista de ficheros que contienen los datos de ésta, a ser usados en el proceso de la transacción y
- finalmente determina si la transacción está permitida.

6.4.1.2. Lectura de Datos de Aplicación (comando READ RECORD)

Los datos contenidos en los ficheros y registros (indicados en el AFL, *Application File Locator*) que hacen referencia directa a la aplicación a ejecutar de la tarjeta son solicitados y leídos por el Terminal para realizar las diversas funciones en el proceso de la transacción. Este paso se realiza inmediatamente después de la consecución exitosa del anterior. Si un error impide al Terminal leer los datos de la tarjeta, la transacción se cancela.

6.4.1.3. Autenticación Off-line de Datos (opcional, comando GET CHALLANGE)

Autenticación Off-line de Datos Estáticos

Este tipo de autenticación es realizado por el Terminal haciendo uso de un esquema de firma digital basado en técnicas de clave pública para confirmar la legitimidad de datos críticos residentes en la tarjeta inteligente y que han sido introducidos previamente por el Emisor de la misma; de esta manera, se detecta la posible alteración no autorizada de dichos datos, tras el proceso de personalización de la misma.

La única forma definida de autenticación off-line de datos estáticos es denominada SDA (Static Data Authentication) y requiere de la existencia de una autoridad de certificación, AC, que firma las claves públicas del Emisor de la tarjeta (por ejemplo, el banco Emisor). Cada Terminal conforme con esta especificación debe contener las claves públicas de dicha autoridad de certificación para cada aplicación reconocida por aquel.

La especificación EMV permite que múltiples aplicaciones compartan el mismo juego de claves de públicas de una autoridad de certificación. La relación entre los datos y las claves criptográficas se muestra en la Figura 6.10.

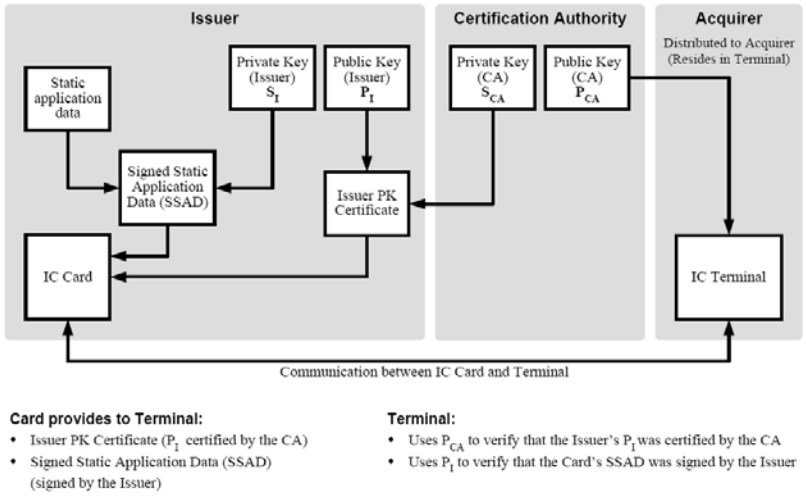

Figura 6.10 Autenticación off-line SDA en EMV

Para soportar SDA, cada Terminal deberá almacenar seis claves públicas de autoridades de certificación por cada proveedor de aplicación y deberá asociar a cada una la información de clave oportuna, de manera que los Terminales en el futuro soporten múltiples algoritmos y permitan una transición apropiada de uno a otro.

De forma resumida los tres pasos iniciales de este esquema de autenticación, visto desde el Terminal, son:

- Obtener la clave pública de la AC.
- Obtiene la clave pública del Emisor de la tarjeta.
- Verificación de la firma sobre los datos de aplicación estáticos

Para soportar SDA, la tarjeta inteligente ha de contener los datos de aplicación estáticos firmados con la clave privada del Emisor de la misma. La clave pública del Emisor debe estar almacenada en dicha tarjeta mediante un certificado de clave pública.

SDA debe usar un algoritmos reversibles según se detalla en la especificación. Para ello prevé el uso de RSA para cifrado y firma digital. Los únicos valores permitidos como exponente de clave público son 3 y $2^{16} + 1$. El criptograma o firma digital resultante es del tamaño del módulo usado. Los límites superiores, de obligado cumplimiento, de tales módulos son 248 para todos los casos; es decir, módulos de las claves públicas de la AC, del Emisor de la tarjeta y de la propia tarjeta (para el caso de cifrado del PIN en la tarjeta se aplicará también este tamaño máximo). El valor del exponente de las claves públicas del Emisor de la tarjeta y la propia tarjeta son determinados por dicho Emisor; en cualquier caso y como queda dicho, tales exponentes, así como el de la clave pública de la AC deberán ser iguales a 3 o $2^{16} + 1$. En cuanto a la generación de claves pública/privada, los sistemas de pagos y las entidades Emisoras son los responsables de la seguridad de los respectivos procesos de tal generación. Como ejemplo de métodos de generación se recomienda el señalado en [Bos95].

En este esquema de autenticación con firma digital con recuperación del mensaje se hará uso de funciones hash de acuerdo a [ISO/IEC 9796-2]. En concreto, se obliga a la utilización de SHA-1 (*Secure Hash Authentication*) que viene estandarizado por [FIPS 180-2] y [ISO/IEC 10118-3]. La aplicación de SHA-1 sobre un mensaje de tamaño arbitrario produce una salida resumen de 20 bytes.

Autenticación Off-line de Datos Dinámicos

Este tipo de autenticación es realizado por el Terminal haciendo uso de un esquema de firma digital basado en técnicas de clave pública para autenticar a la tarjeta inteligente y confirmar la legitimidad de datos críticos residentes en la tarjeta inteligente o los generados por ésta así como los recibidos desde el Terminal, para evitar ataques basados en la falsificación de aquella.

Existen 2 formas de autenticación off-line de datos dinámicos:

- Autenticación de Datos Dinámicos (Dynamic Data Authentication, DDA) ejecutada antes de la fase de análisis de la acción de la tarjeta (card action analysis), donde ésta genera una firma digital sobre los datos generados/residentes llamados datos dinámicos de la tarjeta (ICC Dynamic

Data) y la lista de datos recibidos desde el Terminal, conocidos por DDOL (Dynamic Data Authentication Data Object List).

- Combinación de la anterior, DDA, junto con Generación de Criptograma de Aplicación (Application Cryptogram Generation), CDA, ejecutada como respuesta al primer y segundo comando GENERATE AC (ver más adelante). En el caso de respuestas del tipo TC (*Transaction Certificate*) o ARQC (*Authorisation Request Cryptogram*), la tarjeta genera una firma digital sobre los datos generados/residentes (ICC Dynamic Data) los cuales contienen dichas respuestas, y una número aleatorio generado por el Terminal (CDOL1 o CDOL2).

En el Perfil de Intercambio de Aplicación (*Application Interchange Profile*, AIP), queda definido cuáles de estas opciones soporta la tarjeta; se ilustra en la Figura 6.11.

Meaning
RFU
SDA supported
DDA supported
Cardholder verification is supported
Terminal risk management is to be performed
Issuer authentication is supported [18]
RFU
CDA supported

Figura 6.11 Perfil de la Tarjeta, AIP, en EMV

Al igual que en el caso anterior, este esquema de autenticación requiere de la existencia de una autoridad de certificación, AC, que firma las claves públicas del Emisor de la tarjeta (por ejemplo, el banco/entidad Emisor). Cada Terminal conforme con esta especificación debe contener las claves públicas de dicha autoridad de certificación para cada aplicación reconocida por aquel.

La especificación EMV permite que múltiples aplicaciones compartan el mismo juego de claves de públicas de una autoridad de certificación. La relación entre los datos y las claves criptográficas se muestra en la Figura 6.12.

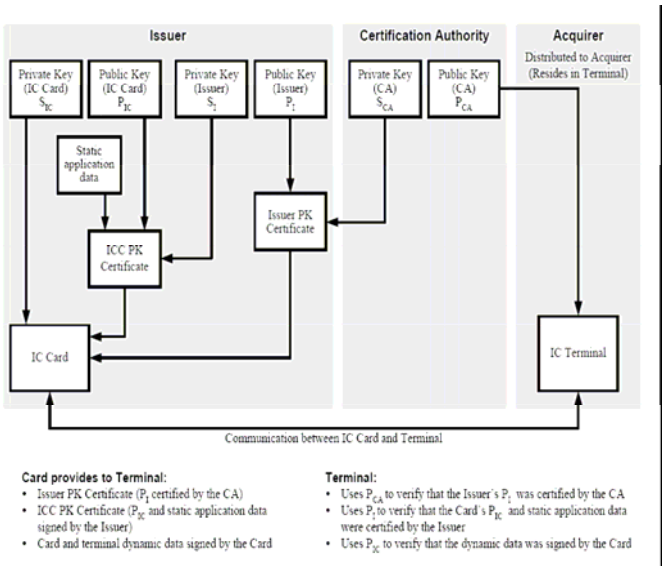

Figura 6.12 Autenticación off-line DDA en EMV

Como también ocurría en el caso de SDA, para soportar autenticación off-line de datos dinámicos, cada Terminal deberá almacenar seis claves públicas de autoridades de certificación por cada proveedor de aplicación y deberá asociar a cada una la información de clave oportuna, de manera que los Terminales en el futuro soporten múltiples algoritmos y permitan una transición apropiada de uno a otro.

De forma resumida los tres pasos iniciales de este esquema de autenticación, visto desde el Terminal, son:

- Obtener la clave pública de la AC.
- Obtener la clave pública del Emisor de la tarjeta.
- Obtener la clave pública de la tarjeta.

Para soportar este tipo de autenticación, la tarjeta deberá disponer de un único par de claves consistente en una clave de privada de firma y la correspondiente pública de verificación. La clave pública de la tarjeta se almacenará en ésta bajo el formato de un certificado de clave pública. En concreto, se hará uso de un esquema de certificación de clave pública de tres capas. Cada clave pública de la tarjeta es certificada por el Emisor de la misma y la AC certifica la de éste último. Esto implica que para la verificación de una firma de la tarjeta, el Terminal primero necesita verificar dos certificados con el objeto de obtener y autenticar la clave pública de la tarjeta, la cual es posteriormente empleada para verificar la firma dinámica de aquella.

En lo relativo a los algoritmos recogidos en esta especificación, tómese en cuenta lo descrito para SDA en el punto anterior.

Intercambio de Comandos y Mensajes

A modo de resumen de las funciones y comandos descritos previamente, se ilustra en la Figura 6.13 un ejemplo de intercambio de comandos y mensajes, donde la autenticación off-line podría llevarse a cabo en una forma opcional.

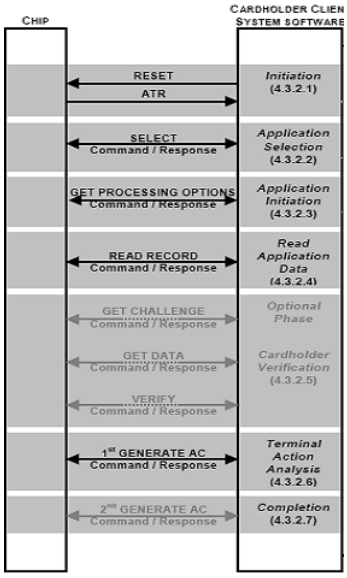

Figura 6.13 Intercambio de comandos para la autenticación off-line según EMV

6.4.1.4. Restricciones del Proceso (opcional, comando GET DATA)

El propósito de esta función es el de determinar el grado de compatibilidad de la aplicación corriendo en el Terminal con la aplicación en la tarjeta y como resultado realizar los ajustes necesarios o, incluso, rechazar la transacción.

El chequeo de compatibilidad consiste en verificar:

- Número de Versión de la Aplicación
- Control de Uso de la Aplicación (válida para compras/pagos nacionales/internacionales, etc.)
- Fechas de Expiración de la Aplicación

6.4.1.5. Verificación del Portador de la Tarjeta (opcional, comandoVERIFY)

La verificación del portador de la tarjeta es realizada para asegurar que la persona que presenta la tarjeta es aquella para quien la aplicación de pago electrónico en la tarjeta fue emitida. La capacidad de la tarjeta debe soportar al menos un método de verificación del usuario, que queda indicado en el AIP. Si es así, el Terminal debe usarla información relativa a la verificación del usuario disponible en la tarjeta para determinar si alguno de los métodos de verificación del usuario, CVM, específicos de cada Emisor, será ejecutado. Con estos métodos se comprobará si el usuario puede o no realizar un pago de débito/crédito, si puede pagar más de una cantidad determinada, si tiene otras restricciones; además, en esta fase se podrá conocer también las reglas referentes a la utilización del PIN previstas para tal usuario.

En relación a la utilización del PIN y su verificación, según las especificaciones de EMV están contempladas las siguientes opciones:

- Verificación por la propia tarjeta del PIN en texto claro.
- Verificación por la propia tarjeta del PIN en texto claro, y firma manuscrita del usuario.
- Verificación del PIN cifrado on-line.
- Verificación por la propia tarjeta del PIN cifrado.
- Verificación por la propia tarjeta del PIN cifrado, y firma manuscrita del usuario.
- No utilización de PIN (firma manuscrita).

La correcta consecución de cualquiera de estas opciones, sólo será posible si el Terminal está preparado para soportarlas.

6.4.1.6. Gestión del Riesgo en el Terminal (opcional)

Esta función, que podría realizarse de forma paralela a los pasos opcionales descritos anteriormente, se centra en la parte de gestión del riesgo que puede asumir el Terminal, con el objeto de proteger contra posibles fraudes al Adquiriente, al Emisor y al sistema. En ella, se precisa una autorización positiva del Emisor para transacciones de gran valor y asegura que las transacciones se realizan on-line periódicamente para proteger contra ciertas amenazas que podrían ser no detectadas en un entorno local u off-line.

Para poder llevar a cabo esta función, la tarjeta deberá tener configurado su AIP para tal efecto y, por tanto, el Terminal debe tener conectividad on-line. Pero más allá, con el objeto de reforzar la seguridad, el Terminal podría llevar a cabo esta funcionalidad incluso cuando en la tarjeta no está prescrita esta condición.

La gestión del riesgo del Terminal consiste en (ver detalles en [EMV04-3]):

- Chequeo del límite inferior (*floor limit*): la suma de las operaciones realizadas por desde una misma tarjeta, no superan un valor monetario determinado.
- Selección de la transacción aleatoria para su procesamiento on-line.

- Chequeo de la velocidad: permite a un Emisor forzar una autenticación on-line después de un determinado número de transacciones off-line.

6.4.1.7. Análisis de la Acción del Terminal (1er comando GENERATE AC)

Una vez que la gestión del riesgo en el Terminal y las funciones de la aplicación normal relativas a una transacción han sido completadas, éste realiza la primera decisión. Ésta podría consistir en la aprobación/declinación off-line de la transacción o redireccionarla on-line. En este punto del flujo de la transacción podría ocurrir:

- Si la decisión es proceder off-line, el Terminal genera un comando GENERATE AC, esperando una respuesta de la tarjeta que contiene TC (*Transaction Certificate*).

- Si la decisión es proceder on-line, el Terminal genera un comando GENERATE AC, esperando una respuesta de la tarjeta que contiene ARQC (*Authorisation Request Cryptogram*).

- Si la decisión es declinar la transacción, el Terminal genera un comando GENERATE AC, esperando una respuesta de la tarjeta que contiene AAC (*Application Authentication Cryptogram*). Esta respuesta podría venir motivada por ciertas restricciones impuestas por las que, por ejemplo, la aplicación en la tarjeta sólo permitiera trabajar con ciertas categorías de comercios.

Ha de notarse que una decisión off-line no tiene porqué ser definitiva. Como resultado de una posterior gestión de riesgo de la tarjeta (*card risk management*) ante la petición de un TC por parte del Terminal, la tarjeta podría responder un AAC, o incluso un ARQC . En este sentido, la propia tarjeta estaría forzando una autenticación on-line.

En la Figura 6.14, se muestra el diagrama de flujo abreviado, en el que se incluyen tanto las funciones de análisis de actuación que han de llevar a cabo tanto el Terminal como la tarjeta, circunstancia que se explica en el próximo punto.

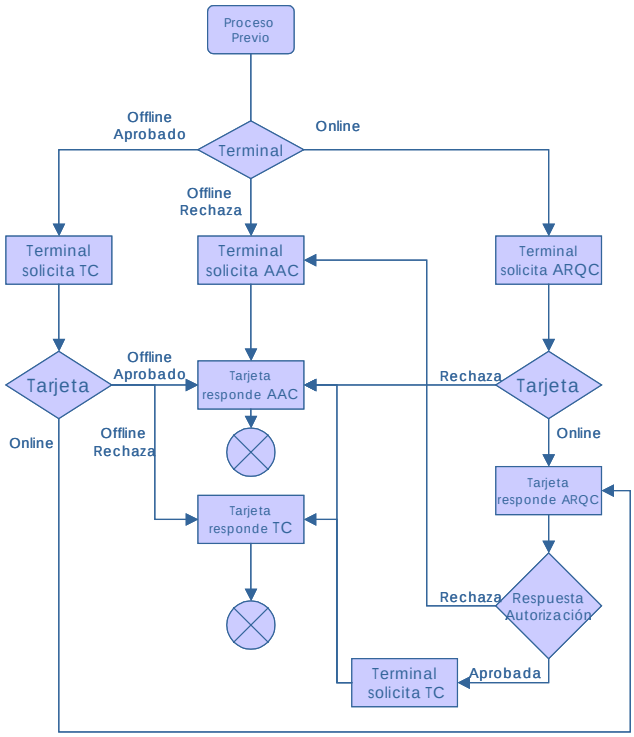

Figura 6.14 Flujo de decisión sobre el tipo de autenticación en EMV

6.4.1.8. Análisis de Acción de la Tarjeta

La tarjeta realiza su propia gestión del riesgo con el objeto de proteger al Emisor de posibles fraudes. Los detalles de los algoritmos que realizan esta gestión dentro de la tarjeta son específicos de cada Emisor y están fuera del alcance de las especificaciones EMV. Como resultado de este proceso, la tarjeta puede decidir completar la transacción on-line u off-line o declinarla. Adicionalmente, la tarjeta podría decidir que un Mensaje de Aviso (*advice message*) fuese enviado al Emisor para informar al mismo de una circunstancia excepcional, por ejemplo cuando se excede el número de intentos de introducción del PIN.

La decisión on-line/off-line es especificada en la respuesta al comando GENERATE AC, devolviendo alguno de los criptogramas de aplicación (*application cryptograms*): TC, ARQC o AAC, tal como se describió en el punto anterior. Por lo tanto, esta función es aplicable a todas las transacciones. Si la tarjeta lleva a cabo cualquier tipo de test para la gestión del riesgo, esto permanece transparente al Terminal.

6.4.1.9. Proceso de Autenticación On-line

Por tratarse esta variante de máximo interés en este capítulo para nuestro trabajo, en tanto que sobre este esquema se pretende aplicar el Marco de Autenticación resultado de esta tesis, dedicamos una sección (6.4.2) ampliada y con posterioridad en este documento.

6.4.1.10. Proceso de Scripts del Emisor a la Tarjeta (opcional)

Un Emisor podría generar comandos *scripts* para ser entregados a la tarjeta por el Terminal, con el objeto de realizar funciones que no son necesariamente relevantes a la transacción vigente pero son importantes para la continuidad de las funcionalidades de la aplicación alojada en la tarjeta.

Múltiples códigos *scripts* podrían ser provistos en una respuesta de autorización y cada uno podría contener un conjunto de comandos *scripts* del Emisor. Esta opción está prevista para permitir que aquellas funciones que no son objeto de la especificación EMV puedan ser incorporadas. El desbloqueo de un PIN podría ser un ejemplo de ello, el cual podría ser realizado indistintamente por emisores o sistemas de pagos.

Un *script* podría contener comandos no conocidos por el Terminal (idealmente debería ser así desde el punto de vista de la seguridad), pero éste debería igualmente entregarlos a la tarjeta.

6.4.1.11. Finalización

Con esta función finaliza el flujo de la transacción y el procesamiento que implica. El Terminal siempre realiza esta función a menos que la transacción termine prematuramente como consecuencia de algún error. Ésta es siempre la última función correspondiente a la transacción, aunque ha de señalarse que el procesado de *scripts*, tal como queda referido más arriba, podría realizarse posteriormente.

La tarjeta indicará su disponibilidad a finalizar la transacción mediante la respuesta con TC o AAC, tanto para el primer como segundo comando GENERATE AC emitido por el Terminal. Si el Terminal decide continuar on-line, la finalización se llevará acabo cuando el segundo comando GENERATE AC sea emitido.

6.4.2. Autenticación On-line

El proceso de autenticación on-line es llevado a cabo para asegurar que el Emisor puede inspeccionar y autorizar/ declinar las transacciones que están fuera de los límites de riesgos definidos por él mismo, el sistema de pago o el Adquiriente. Como se ha mencionado dicho proceso se llevará a cabo si la tarjeta devuelve un ARQC en respuesta al primer comando GENERATE AC de una transacción.

En general esta funcionalidad es la misma que la llevada a cabo en las transacciones con tarjetas magnéticas. El ARQC podría ser enviado en el mensaje de solicitud de autorización. El ARQC es un criptograma generado por la tarjeta con los datos de la transacción haciendo uso de la clave del Emisor almacenada en ésta y conocida por el sistema de autorización del Emisor. El Emisor utiliza tal clave para autenticar el ARQC y con ello autenticar la tarjeta. Este proceso es conocido como la "Autenticación on-line de la tarjeta" o simplemente "autenticación de la tarjeta". Como siguiente paso, el Emisor genera un criptograma, ARPC, con ciertos datos y lo incluye en el mensaje de respuesta a la autorización, o bien, la tarjeta ya lo conoce. Este criptograma es enviado al Terminal en tal respuesta como parte de los Datos de Autenticación del Emisor

(*Issuer Authentication Data*). El Terminal proporciona estos datos a la tarjeta en el comando EXTERNAL AUTHENTICATE (o en el segundo comando GENERATE AC). La tarjeta podría hacer uso de dichos datos de autenticación del Emisor para autenticarle y tener la certeza de que el mensaje fue realmente originado por aquel. Para que este proceso sea posible, el AIP debe estar configurado de manera que la autenticación del Emisor esté permitida (Figura 6.11). Obsérvese en el diagrama de flujo anterior, Figura 6.14, la bifurcaciones en las funciones de decisión que han de producirse para completar un proceso de autenticación on-line.

Intercambio de Comandos y Mensajes

A modo de resumen de las funciones y comandos descritos previamente, se ilustra en la Figura 6.15 un ejemplo de intercambio de comandos y mensajes podrían llevarse a cabo en una autenticación on-line.

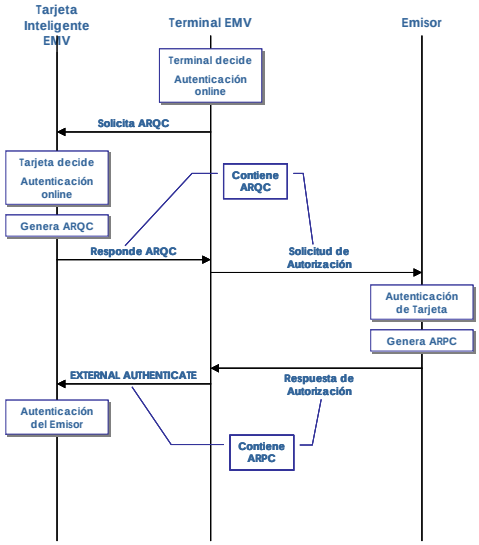

Figura 6.15 Autenticación on-line en EMV

6.4.2.1. Generación de ARQC y de ARPC

La especificación EMV se limita a recomendar unos métodos para la generación de criptogramas de aplicación y por tanto no son de obligado cumplimiento. Dicha especificación define tales métodos para los criptogramas TC, ARQC o AAC, generados por la tarjeta, así como ARPC (*Authorisation Response Cryptogram*), generado por el Emisor, y a verificar por aquella.

En este apartado se hará referencia en todo momento en la generación de ARQC, aunque aplicable al resto de criptogramas, con el fin de centrar la explicación en el proceso de autenticación on-line, de significativo interés en nuestro trabajo.

Un criptograma de aplicación AC se genera mediante una función MAC (Message Authentication Code) sobre ciertos datos, que son transmitidos desde el Terminal a la tarjeta en el comando GENERATE AC y accedidos internamente por ésta última. El conjunto mínimo de datos recomendados para la generación de AC, se muestra en la Tabla 6.2.

Value	Source
Amount, Authorised (Numeric)	Terminal
Amount, Other (Numeric)	Terminal
Terminal Country Code	Terminal
Terminal Verification Results	Terminal
Transaction Currency Code	Terminal
Transaction Date	Terminal
Transaction Type	Terminal
Unpredictable Number	Terminal
Application Interchange Profile	ICC
Application Transaction Counter	ICC

Tabla 6.2 Conjunto mínimo de datos recomendado para la generación de un criptograma de aplicación, AC

6.4.2.2. Algoritmo para la generación de ARQC

El algoritmo para la generación de ARQC, llevado a cabo en la propia tarjeta, toma como únicas entradas los datos seleccionados y la clave maestra específica para la generación de AC almacenada en dicha tarjeta, MK_{AC} de 16 bytes, para computar un criptograma resultante de 8 bytes, según:

- Derivación de Clave de Sesión: la clave de sesión de SK_{AC} de 16 bytes se obtiene a partir de MK_{AC} y del contador de transacción ATC (2 bytes) de la tarjeta (ver detalles en [EMV04-2]).
    - $SK_{AC} := f(MK_{AC}, ATC)$
- Entrada:
    - Datos seleccionados, Z
- Algoritmo: genera el criptograma resultante de 8 bytes aplicando una función MAC según [ISO/IEC 9797-1] cifrando con 3DES [ISO 11568-2] en modo CBC [ISO/IEC 10116] con la clave de sesión SKAC derivada en el paso anterior, sobre los datos seleccionados Z.
    - ARQC:= MAC: = MAC $(SK_{AC})[Z]$

6.4.2.3. Algoritmos para la generación de ARPC

Los criptogramas ARPC (8 bytes o 4 bytes) son generados por el Emisor como respuestas a ARQC y que deben servir para la autenticación de éste frente a la tarjeta. Son dos los métodos previstos en EMV para llevar a cabo dicha generación:

Método 1

- Entradas:
  - Petición ARQC de 8 bytes enviada por la tarjeta
  - Código de Respuesta de Autorización (*Authorisation Response Code*, ARC) de 2 bytes.
- Algoritmo:
  - Relleno de ARC con 6 bytes de 0, resultando X de 8 bytes.
  - Computar Y: = ARQC $\oplus$X.
  - Computar: ARPC := 3DES(SK_{AC})[Y] (8 bytes)

Método 2

- Entradas:
  - Petición ARQC de 8 bytes enviada por la tarjeta.
  - Actualización del Estado de la Tarjeta (*Card Status Update*, CSU) de 4 bytes.
  - Datos de Autenticación Propietarios, de 0 a 8 bytes en binario.

- Algoritmo:
  - Concatenar: Y: = ARQC || CSU || Datos de Autenticación Propietarios
  - Computar ARPC 4 bytes mediante MAC, según el algoritmo 3 de [ISO/IEC 9797-1] con s=4
    - ARPC: = MAC: = MAC (SK_{AC})[Y]
  - Generar los Datos de Autenticación del Emisor (*Issuer Authentication Data, IAD*)
    - IAD: = ARPC || CSU || Datos de Autenticación Propietarios

6.5. Aplicación del Marco de Autenticación para Tarjetas Inteligentes

Como se ha mencionado previamente, uno de los objetivos de nuestro trabajo, y que ha de quedar reflejado en este capítulo, es el demostrar la aplicabilidad de nuestro Marco de Autenticación para tarjetas inteligentes en escenarios de pago electrónico en entornos inalámbricos. En este caso, y como viene describiéndose en este capítulo, se ha tomado como referencia las especificaciones descritas en EMV. En concreto, dicha aplicabilidad tiene sentido en el caso que, durante el proceso de autenticación, ésta se realiza on-line tal como se describe en el apartado 6.4.2 del presente documento. Según nuestra propuesta, una comunicación remota en capa 2 –basada en nuestra Arquitectura de Protocolos de Autenticación– se ha de producir entre la tarjeta y el servidor de

autenticación remoto, alojado en el dominio del Emisor. Siguiendo el enfoque marcado por nuestro Modelo Extendido de Autenticación, tal conexión remota a través de un sistema en red deberá realizarse netamente entre la tarjeta y tal servidor, según se detalla en la Figura 3.9.

Por tanto, la aplicación efectiva de nuestro Marco de Autenticación tiene cabida a partir del paso en el que el Terminal realiza el análisis de la acción a realizar y efectúa la decisión de proceder con una autenticación on-line. Los detalles y criterios en los que se basa el Terminal para llevar a cabo tal proceso de decisión no afectan en ningún punto al propósito de aplicabilidad aquí presentado. Por ello, tales detalles y criterios quedan fuera de alcance de este documento, pudiéndose encontrar ampliamente descritos en [EMV04-3].

Proceso Previo

El intercambio de comandos y mensajes realizados en el proceso previo a la autenticación on-line, no se ven afectados por la aplicación de nuestro modelo. Detalles de los mismos pueden encontrarse en el apartado 6.4.

Autenticación on-line

A continuación se describen las acciones e intercambios de comandos y mensajes, que se suceden para llevar a cabo la autenticación on-line referida en EMV para el pago electrónico con tarjetas inteligentes, sobre la base de nuestro Marco de Autenticación y tomando como referencia la descripción genérica del procedimiento de autenticación previsto en dichas especificaciones y que quedó ilustrado en la Figura 6.15.

En la Figura 6.16 se representa el protocolo completo, como resultado de la aplicación de nuestros modelos y arquitectura propuestos; como ejemplo, se ha representado el caso particular en el que el proceso de autenticación on-line mutua culmina exitosamente. Obsérvese que en las descripciones realizadas a continuación los términos comandos y paquetes son utilizados indistintamente, al hacer referencia a la comunicación de la tarjeta con el resto del sistema.

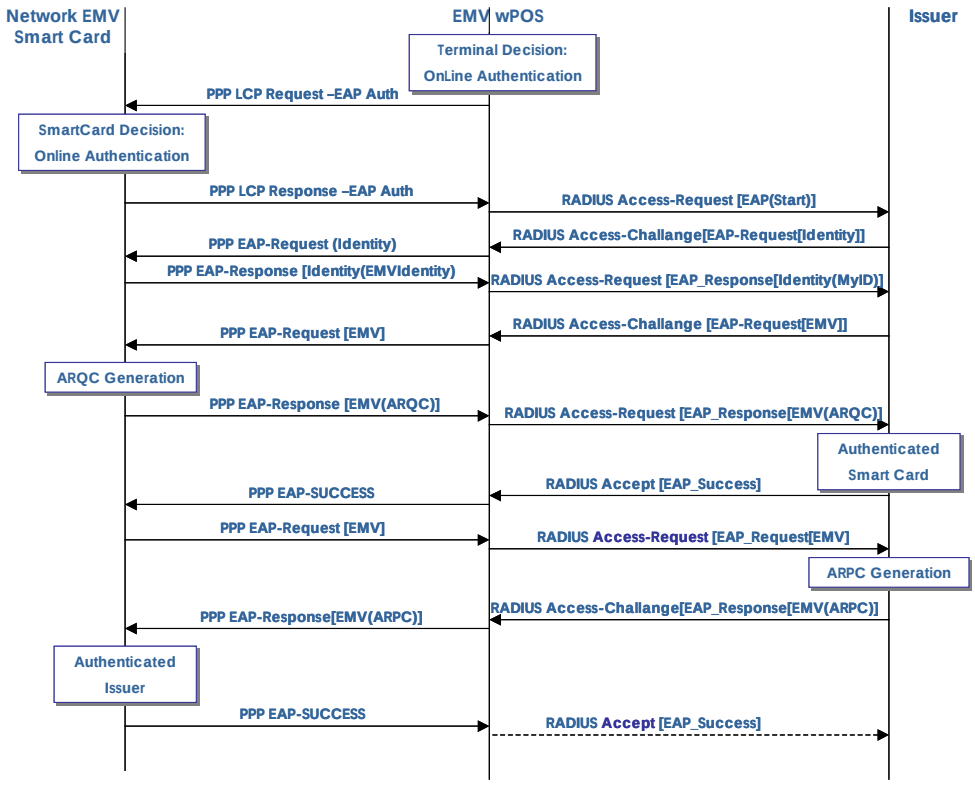

Figura 6.16 Aplicación del nuevo Marco de Autenticación para Tarjetas Inteligentes en escenarios de Pago Electrónico entornos inalámbricos

`PPP-LCP Request EAP-Auth`

Una vez que el Terminal decide llevar a cabo una autenticación on-line (para más detalles se remite al lector al apartado 6.4), dado que participa en el proceso de autenticación en el rol de autenticador inicia la negociación del tipo de autenticación basada en EAP sobre un enlace PPP LCP mediante las opciones de configuración (*Configuration Options*) que prevé este protocolo (otras opciones de configuración para el establecimiento del enlace LCP podrían incluirse en el mismo paquete/ comando) . Para ello envía el mensaje `PPP-LCP Request EAP-Auth`, que consiste en el mapeo de un paquete PPP LCP sobre un comando APDU, en la forma que se detalló en el apartado 4.2.3.

`PPP-LCP Response EAP-Auth`

Si el resultado de la decisión de la tarjeta inteligente es proceder con una autenticación on-line, tal como se define en EMV, debería responder al paquete de forma positiva con el mensaje `PPP-LCP Response EAP-Auth`, por el que el Terminal autenticador deberá interpretar que la tarjeta admite la autenticación on-line, y más allá, admite realizarla sobre el protocolo EAP, respondiendo al Marco de Autenticación propuesto en nuestro trabajo.

RADIUS Access-Request [EAP(Start)]

El Terminal EMV solicita mediante este mensaje al servidor RADIUS, el inicio por parte del mismo de un proceso de autenticación basado en EAP. El Terminal autenticador encapsulará desde este momento todos los mensajes EAP provenientes de la tarjeta según se especifica [Abo03]; por tanto, serán atributos en los mensajes de RADIUS sobre una conexión UDP/IP hacia el Emisor, donde un servidor RADIUS permanece a la escucha.

RADIUS Access-Challange[EAP-Request[Identity]]

Al recibir el mensaje RADIUS Access-Request [EAP(Start)], el servidor RADIUS solicita la identidad del *supplicant* y recibirá la respuesta en el mensaje RADIUS Access-Request [EAP-Response[Identity(EMVIdentity)]. Para mantener la coherencia con las especificaciones del protocolo EAP, se han incluido los mensajes de petición y respuesta desde el Terminal PPP EAP-Request [Identity] y PPP EAP-Response [Identity(EMVIdentity)] respectivamente.

Así, la tarjeta podría disponer, de una identidad específica en el marco de trabajo de EMV, que la identifica frente al servidor de autenticación del Emisor, en todo momento basada en EAP y respetuosa con nuestro Marco de Autenticación. La respuesta obtenida de la tarjeta será encapsulada como atributo del mensaje RADIUS.

RADIUS Access-Challange[EAP-Request[EMV]]

Una vez que el servidor de autenticación del Emisor comprueba la identidad de la tarjeta, en el rol de solicitante de autenticación, y da su conformidad para proceder con el proceso de autenticación on-line extremo a extremo sobre el protocolo EAP, responde con el mensaje RADIUS Access-Challange[EAP-Request[EMV]]; este mensaje, dirigido hacia el autenticador, servirá como el auténtico disparador del proceso de autenticación on-line de EMV, según se explica a continuación.

PPP EAP Request [EMV]

A la recepción del mensaje RADIUS Access-Challange[EAP-Request[EMV]], el Terminal autenticador tiene la confirmación por parte del Emisor de que la tarjeta puede comenzar un proceso de autenticación on-line de la misma, basándose en la Arquitectura de Protocolos de Autenticación elaborada sobre nuestros modelos. Para ello, generará el paquete PPP-EAP Request [EMV], según las técnicas de mapeo descritas en este documento, apartado 4.2.3. El campo *Code* tomará el valor 0x01 para la creación de esta solicitud. Este puede ser considerado como el primer paquete, en el que un mensaje concebido por las especificaciones EMV para las tarjetas inteligentes ISO7816, es *integrado* de forma transparente en un protocolo de redes. En este sentido, y como se ha mencionado, EAP será el protocolo de capa 2, para su transporte de extremo a extremo.

`PPP EAP-Response [EMV(ARQC)]`

Tal como prevén las especificaciones EMV, al recibir la tarjeta inteligente el mensaje `PPP EAP-Request[EMV]`, ésta procederá con la generación del criptograma ARQC tal como esta previsto en las mismas y queda descrito en nuestro trabajo (apartado 6.4.2.1). El objetivo perseguido es que la información contenida en el criptograma original ARQC sea transportado hasta el servidor de autenticación en el Emisor, que deberá proceder con la autenticación on-line de la tarjeta, sobre la base de la información recibida. Para ello, la tarjeta inteligente integrará el criptograma ARQC en el paquete `PPP EAP-Response [EMV(ARQC)]`para llevar a cabo su transporte según nuestra arquitectura.

`RADIUS Access-Request[EAP-Response[EMV(ARQC)]]`

De acuerdo con [Abo03], cuando el autenticador recibe una respuesta procedente del solicitante de autenticación transportada sobre EAP (EAP Response), la encapsula en una petición de acceso de RADIUS; como resultado, el Terminal envía el mensaje `RADIUS Access-Request[EAP-Response[EMV(ARQC)]]`hacia el servidor de autenticación, con el objeto de autenticar la tarjeta a partir del criptograma ARQC generado por la misma, tal como se prevé en EMV.

`RADIUS Accept [EAP-Success]`

En el ejemplo representado en la Figura 6.16, la tarjeta es correctamente autenticada por el Emisor, a través de su servidor RADIUS que responde al Terminal con el mensaje `RADIUS Accept [EAP-Success]`; en caso contrario, tal servidor debería informar del fallo en la validación del criptograma ARQC enviado por la tarjeta, mediante un mensaje similar: `RADIUS Reject [EAP-Failure]`.

`PPP EAP-Success`

En el caso de una validación positiva del criptograma ARQC recibido del Emisor, el Terminal hará llegar dicha información a la tarjeta mediante el mensaje `PPP EAP-Success,` comunicando el éxito de la autenticación on-line. En caso de validación negativa, se produciría la comunicación de una autenticación fallida mediante un mensaje `PPP EAP-Failure.` Obsérvese por otro lado, que para inclusión de EAP en este esquema con rigor, ciertas respuestas del Emisor, como en el caso de `Success`, no pueden *reutilizarse* para enviar respuestas a la tarjeta, lo que ahorraría mensajes en el procedimiento de autenticación. Esta restricción queda contemplada en [Abo04], y en este sentido ha sido concebida la presente aplicación. Una vez que la tarjeta recibe `PPP EAP-Success,` puede activar el proceso inverso para autenticar al Emisor. Para ello, envía el mensaje que se describe a continuación.

`PPP EAP-Request [EMV]`

Con el objeto de iniciar la autenticación del servidor por parte de la tarjeta, ésta envía al Terminal la petición `PPP EAP-Request [EMV]`, esperando del servidor el criptograma ARPC para su validación.

`RADIUS Access-Request[EAP-Request[EMV]]`

Cuando el Terminal recibe el mensaje `PPP EAP-Request[EMV]]`desde la tarjeta, lo encapsula en un nuevo mensaje de petición al servidor `RADIUS Access-Request[EAP-Resquest[EMV]]`con el objeto de solicitar de forma asíncrona al Emisor el criptograma respuesta ARPC, según se describe en el apartado 6.3.2.1, y que deberá ser encapsulado en el siguiente mensaje.

`RADIUS Access-Response[EAP-Response[EMV(ARPC)]]`

Tras la solicitud y generación del criptograma ARPC, el Emisor responderá con el mensaje `RADIUS Access-Response[EAP-Response[EMV(ARPC)]]`, en el que tal criptograma va integrado en una respuesta del protocolo EAP, y deberá llegar hasta la tarjeta con el objeto de que ésta autentique al Emisor, completando el ciclo de la autenticación mutua on-line.

`PPP EAP-Response[EMV(ARPC)]`

Mediante este mensaje, el Terminal envía a la tarjeta la respuesta del Emisor para proceder con la autenticación del mismo, en función del criptograma ARPC recibido en dicho mensaje. Este paquete se formará según las técnicas de mapeo descritas en este documento, apartado 4.2.3. El campo *Code* tomará el valor 0x02 para la creación de esta respuesta.

`PPP EAP-Success`

En el caso de una validación positiva del criptograma ARPC recibido del Emisor, la tarjeta se verá en disposición de emitir el mensaje `PPP EAP-Success,` comunicando el éxito de la autenticación on-line de dicho Emisor, según se prevé en EMV. En caso de validación negativa, se produciría la comunicación de una autenticación fallida mediante un mensaje `PPP-EAP Failure.`

`RAIDUS Accept [EAP-Success]`

Finalmente, el Terminal será el encargado de encapsular el mensaje `EAP-SUCCESS/FAILURE` en un paquete del protocolo RADIUS para su envío al servidor de autenticación y consecuente información de éste.

6.6. Método EAP-EMV

La creación formal de un Método EAP de tipo EMV (EAP-EMV, EAP-type=EMV), en principio queda fuera del alcance de este trabajo y se pospone para trabajos futuros. No obstante el protocolo aplicado sobre el escenario de autenticación on-line con tarjetas inteligentes EMV y que se ha descrito en detalle en este capítulo facilita en gran medida la definición del tal método. Por completar esta idea, baste decir que la generación de ARQC en la tarjeta y ARPC en el Emisor, constituirían en sí mismo el núcleo de este Método EAP. La fijación de los valores de los Types y la concreción del contenido de los mensajes EMV, podrán formar parte de un proceso de estandarización como borrador de internet (Internet-Draft), y que como se ha mencionado podría ser objeto de trabajos posteriores.

6.7. Conclusiones de la Aplicación a escenarios de Pago Electrónico en entornos Inalámbricos

En este capítulo hemos descrito la aplicación del nuevo Marco de Autenticación para Tarjetas Inteligentes en Red para escenarios de pago electrónico en entornos inalámbricos, dando cumplimiento con ello al segundo de los objetivos principales planteados al inicio de esta tesis y demostrando su aplicabilidad y utilidad, en términos prácticos.

Con esta aplicación a escenarios de pago electrónico conseguimos demostrar las ventajas que el Marco de Referencia aplicado presenta, en tanto que facilita la migración *suave* de los mecanismos de autenticación previstos en las especificaciones EMV –inicialmente diseñados bajo enfoque orientado al medio de acceso que comparte la tarjeta inteligente ISO 7816 y el Terminal– hacia la futura generación de tarjetas inteligentes. La utilización de protocolos de seguridad estandarizados para entornos de red como EAP, y las ventajas que éste presenta para su implementación en la tarjeta inteligente sin necesidad de una pila de protocolos TCP/IP completa, refuerzan el resultado aquí obtenido. Por último, el protocolo y mecanismos descritos en este capítulo son claramente aplicables a las futuras tarjetas inteligentes en red (*network smart cards*), respondiendo con ello a nuestros objetivos.

Capítulo 7.

Conclusiones y Trabajos Futuros

7. Conclusiones y Trabajo Futuros

7.1. Conclusiones

La importancia de los mecanismos y técnicas orientados al fortalecimiento de las garantías de seguridad de la Información y de las Comunicaciones resulta en estos momentos incuestionable. Buena prueba de ello son los esfuerzos y recursos que, desde distintos planos de la sociedad, se vienen empleando en los últimas décadas, en aras de amortiguar los defectos y vulnerabilidades inherentes al trasiego de la información digital. En este contexto, la relevancia de una autenticación fiable de dispositivos y usuarios queda también patente en una diversidad de aspectos cotidianos que abarca desde lo organizacional hasta lo institucional, pasando por un amplio espectro de sistemas de distinta índole. Por sus cualidades y ventajas como módulo o *token* criptográfico, a menudo derivadas de su propia naturaleza, la tarjeta inteligente ha desarrollado un papel fundamental en la evolución de la autenticación de usuarios.

Sin embargo, a lo largo de esta tesis ha quedado patente el proceso de transformación que está atravesando actualmente el concepto de tarjeta inteligente. Así, de su utilización como dispositivo pasivo para dar soporte al usuario en términos de computación de algoritmos criptográficos de autenticación, de almacén de credenciales de seguridad o, como *autenticador* del portador de la tarjeta (p.e. en un proceso de autenticación *off-line* del PIN de usuario), pasará a ser un dispositivo con conectividad en red, como si se tratara un *hos*t común. Esta funcionalidad –que tendría obviamente un impacto sobre el interfaz de comunicación–, así como otras relativas a distintos planos tanto de la tarjeta inteligente como del terminal, conformarían lo que se ha dado en llamar la *Nueva Generación de Tarjetas Inteligentes*.

Con esta evolución, se abre un repertorio de posibilidades, atribuciones e implicaciones en el plano de la seguridad, que se expanden transversalmente desde el momento que dicha tarjeta se conecta en red. Por tanto, el papel relevante que adoptarán las tarjetas inteligentes bajo este nuevo prisma y el impacto en términos de seguridad que de esta tendencia se deriva, son de especial interés en nuestro estudio y análisis, y conforman el núcleo de nuestro trabajo. De esta manera, esta tesis se ha centrado inicialmente en las soluciones para la integración de forma factible de la tarjeta inteligente en la red, y más concretamente, se ha focalizado en los mecanismos de autenticación que ha de soportar la tarjeta para poder acceder de forma autorizada a dicha red. Por tanto, por *integración de la tarjeta inteligente en la red*, se ha considerado en el contexto de esta tesis como la capacidad de ésta para comunicarse en términos de autenticación remota, a través de la infraestructura de red; entendiendo este hecho, como parte de los primeros pasos en esa evolución hacia una nueva generación de tarjetas inteligentes.

Conviene observar que este hecho no se presenta de forma aislada. Por una lado, la potencia del concepto, cada vez más generalizado, de *all-IP* , sobre una heterogeneidad de tecnologías de infraestructura de red, sumada a la inequívoca cohabitación de una diversidad de redes de acceso, entre las que proliferan las tecnologías inalámbricas y los dispositivos *multimodo*, van a conformar un panorama global del que las tarjetas inteligentes, actuales y futuras, deben participar y habrán de integrarse de la forma más

transparentemente posible. Es necesario apuntar, que en esta coyuntura la tarjeta no es ajena a las limitaciones computacionales de las que, para ciertos usos, sigue y seguirá adoleciendo.

Como antecedente en la investigación, se ha estudiado el diseño tradicional de los protocolos de autenticación remota para las tarjetas inteligentes y se ha propuesto un modelo que nos permite analizar el enfoque que se le ha dado a estos diseños y estudiar las circunstancias que los justifican. Como conclusión de estos análisis, se señalan dos aspectos relevantes. De un lado, en tales diseños la tarjeta carece de entidad propia o autonomía en el proceso de autenticación, y por tanto, participan tangencialmente en el proceso como soporte al usuario o al terminal. De otro lado, estos diseños no se realizan bajo una perspectiva de atomicidad; es decir, el protocolo al completo no se diseña exclusivamente para la tarjeta, sino que las funcionalidades de autenticación están claramente divididas entre el terminal, sobre el que recaen parte de estas funcionalidades, y la propia tarjeta. El estado de la cuestión en esta materia revela esta circunstancia, que en nuestra opinión debe ser evitada por motivos claros de seguridad. La consideración inicial de un terminal no confiable se presenta como una premisa necesaria en el análisis posterior.

Como otro de los primeros pasos en la investigación y ante el hecho ineludible –a medio/largo plazo– de la integración de la tarjeta inteligente en la red, se ha pretendido dar respuesta a uno de los cuestionamientos generados en el seno de esta tesis: hacia dónde evoluciona *esa red*. En concreto, por ser el terminal y red de acceso las entidades con las que entra en comunicación directa la tarjeta inteligente, han demandado en nuestro trabajo de la atención oportuna, con la pretensión de identificar la convergencia tecnológica en la que habrán de confluir estas tecnologías. Al tratarse la tarjeta inteligente de un dispositivo portátil, cabe esperar su utilización en múltiples escenarios. En una primera aproximación, se han considerado los entornos públicos como los más representativos de la interacción con dispositivos lectores, a priori, no confiables. En este sentido, las *redes locales*, especialmente las inalámbricas públicas o PWLAN, permitirían el acceso ubicuo a la red de una variedad de dispositivos, y entre ellos podrían estar las tarjetas inteligentes. Las ventajas de la consideración de redes locales para al acceso a los servicios de autenticación por parte de estos dispositivos se han señalado en este documento y pueden resumirse en: se trata de una red en capa 2 según el Modelo de Referencia OSI, lo que permitiría una integración de la tarjeta inteligente en la red para la dotación de ciertos servicios, con una pila de protocolos más ligera; los mecanismos y recursos en esta capa podrían ser lo suficientemente robustos como para implementar un adecuado servicio de autenticación; esto no excluye la posibilidad de la implementación de otros de capas superiores, cuando así fuese requerido; los primeros avances en las tarjetas inteligentes en red, han ido encaminados hacia la provisión de una capa 2 tipo *Ethernet* en las actuales tarjetas inteligentes ISO 7816; y por último, permite una reconsideración sobre el papel del terminal, a priori no confiable, como dispositivo de la propia red local de acceso.

En este contexto, se contempla de forma novedosa el problema de la autenticación remota y autónoma de la tarjeta inteligente desde una perspectiva global, que dé cabida al conjunto de convergencias tecnológicas (dispositivos y redes de acceso) previstas, y por ello ha partido hacia la búsqueda de un nuevo *Marco de Referencia* que sirva como base de estudio y dinamizador de soluciones aplicables.

Con tal propósito, esta tesis ha apostado por el estudio inicial del comportamiento de una variedad de dispositivos ante la autenticación, tratando de identificar el caso que presenta las condiciones más favorables para su adopción por parte de la tarjeta inteligente en la red, dadas sus particularidades. El resultado de dicho estudio concluye con la conveniencia de adoptar un *enfoque basado en infraestructura*, según se define en esta tesis, del que se destacan las siguientes características: permite introducir el concepto *tarjeta inteligente en red* para la dotación de un servicio de autenticación, al tiempo que esto favorece el grado de adaptabilidad del diseño del protocolo de autenticación hacia el modo en el que se va a realizar la comunicación; potencia la portabilidad y conectividad de la tarjeta en un entorno interoperable; facilita la adaptación a los servicios o aplicaciones finales; y por último, da cabida a la incorporación del terminal de forma segura al propio esquema de autenticación, quedando supeditado al control de otras entidades.

El enfoque basado en infraestructura para la autenticación de dispositivos toma como mejor ejemplos aquellos casos basados en el estándar IEEE 802.1X, del que se puede inferir un Modelo de Autenticación Genérico, así denominado en nuestro trabajo, que se limita a establecer las relaciones de autenticación que se producen entre las entidades. Éste ha servido como referencia para definir en esta tesis un nuevo modelo: Modelo Extendido de Autenticación, que resuelve la problemática de incorporar en el primero una tarjeta inteligente que desea acceder a los servicios de autenticación en la red. Para completar el sentido y la correcta dimensión del modelo propuesto, se han definido un conjunto de requerimientos de autenticación asociados al mismo, que imponen las condiciones que han de regir las relaciones de autenticación entre las entidades participantes, una de las cuales ahora es la tarjeta inteligente, para garantizar la seguridad del esquema. De esta manera el Modelo Extendido de Autenticación y los Requisitos de Autenticación asociados que hemos propuesto, pueden considerarse como dos de los elementos que componen el *marco de referencia* pretendido y que en esta tesis hemos dado en llamar *Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red*.

Dicho marco incorpora además otros elementos. De un lado, la necesidad de estudiar la seguridad relativa al Modelo Extendido de Autenticación nos obliga a introducir una componente de *análisis* en nuestro Marco de Autenticación. Mediante la inclusión de un nuevo elemento, el Modelo de Confianza Extendido, hemos podido analizar las relaciones de confianza – como base de la seguridad del sistema – entre las entidades interventoras. De otro lado, una componente referida a la *arquitectura* ha sido considerada junto con la del *modelo* y el *análisis*. En esta línea, esta tesis ha propuesto una nueva Arquitectura de Protocolos de Autenticación Remota para tarjetas inteligentes, que supone otro de los elementos constituyentes de dicho marco de referencia, y por tanto coherente con el resto de ellos. Esta arquitectura, que es aplicada en esta tesis para tarjetas ISO 7816, presenta la ventaja de que está basada en protocolos de capa 2, por lo que – por ejemplo– no es necesario conectividad IP, y por tanto no es necesaria la inclusión de una capa de red bajo este enfoque de autenticación. Así, el trabajo aquí realizado puede ser también considerado como un paso hacia las futuras tarjetas en red.

Sin embargo, para una adecuada integración de las actuales tarjetas inteligentes en dicha Arquitectura de Protocolos basada ampliamente en el protocolo EAP (*Extensible Authentication Protocol*) y dar respuesta completa al Modelo Extendido de

Autenticación, ha sido necesario analizar de nuevo el modelado de este protocolo en tarjetas inteligentes. El análisis desarrollado en esta tesis concluye con la contribución de un nuevo Modelo de Multiplexación EAP específico para tarjetas inteligentes y, al mismo tiempo, plenamente respetuoso con los Requisitos de Autenticación aquí formulados; especialmente, atiende al requisito referido a la necesidad de evitar un solicitante de autenticación dividido y por tanto abogando por la atomicidad en el diseño, que culmina con una tarjeta *auto-autenticable*. Nuestro Modelo de Multiplexación EAP específico para tarjetas inteligentes requiere de una capa de adaptación en la pila de protocolos basada en LCP/PPP. Sobre este nuevo modelo para tarjetas inteligentes, ahora la Arquitectura de Protocolos de Autenticación Remota responde plenamente a los modelos referidos. Por tanto, este último es imprescindible para la concepción de nuestro Marco de Autenticación para Tarjetas Inteligentes en Red y se incluye como otro de los elementos basales del mismo. De esta manera, se dan por cumplidos el conjunto de objetivos parciales planteados al inicio de esta tesis, a falta de la fase de diseño e implementación, así como la aplicación a un escenario concreto.

Como continuación de nuestro trabajo, se ha perseguido en esta tesis la implementación de dicha arquitectura, partiendo del interfaz más crítico y en torno al cual se articula el Modelo de Multiplexación EAP para tarjetas inteligentes y, por ende, el Modelo Extendido de Autenticación. Para ello ha sido necesario una metodología de implementación basada en las técnicas de mapeo descritas en este documento. Se aporta en este trabajo de tesis la descripción de dicha metodología y de la programación consecuente en el ámbito de la tarjeta inteligente. Este proceso ha requerido de la selección de los entornos y herramientas de simulación, que ha desembocado en la programación con Java Card de dicho modelo. Como entorno de simulación se ha empleado el que proporciona Java Card 2.1.2 Development Kit, de Sun Microsystems y en especial se ha hecho uso de las herramientas JCWDE y APDUTool.

Para dar cuenta de la factibilidad de la implementación y poder concluir sobre viabilidad de este Marco de Autenticación, se han desarrollado un conjunto de pruebas que conforman la evaluación de las funcionalidades previstas por los protocolos considerados. Estos tests se componen de un conjunto ficheros con código *script*, cada uno de ellos diseñado para chequear las funcionalidades concretas de la implementación, tanto del protocolo LCP/PPP como del protocolo EAP. A modo de conclusión a esta fase de análisis de resultados de la implementación, destacamos la validación de los modelos a la vista de los resultados obtenidos.

Con el objeto de contribuir en términos de practicidad y aplicabilidad con la elaboración de esta tesis, se ha completado con una última fase de aplicación a un escenario realista de *pago electrónico con tarjetas inteligentes en entornos inalámbricos*. El pago electrónico con tarjeta inteligente comienza a acumular una trayectoria sólida y, más allá, proyecta a futuro unas posibilidades de implantación masiva, normalmente dinamizadas por el motor de los intereses de las entidades de servicios financieros y bancarios. Por todo ello, se ha demostrado cómo es posible incorporar la autenticación on-line para tarjetas inteligentes ISO 7816 –definida en las especificaciones EMV al efecto–, en nuestro Marco de Autenticación con un impacto mínimo o nulo del protocolo, pero aprovechando las claras ventajas que dicho marco ofrece. Con esto se culmina el segundo de los objetivos principales que se platearon al inicio, referidos a la viabilidad y sentido práctico de dicho marco y por ende, de esta tesis doctoral.

En resumen, las ventajas de este nuevo *Marco de Autenticación de Autenticación para Tarjetas Inteligentes en Red* para el diseño de esquemas de autenticación en una diversidad de escenarios y de aplicaciones, se derivan de tres importantes consideraciones, realizadas en el transcurso de esta tesis: diseño atómico del protocolo de autenticación en la tarjeta; con la consecuente autonomía e independencia en el proceso de autenticación (auto-autenticable) y por tanto en pos de la seguridad; la consideración de redes locales para al acceso en capa 2 a los servicios de autenticación por parte de la tarjeta inteligente, cuya conveniencia ya ha sido remarcada; y por último, un diseño bajo un *enfoque basado en infraestructura*, cuyas ventajas también han sido enunciadas.

En contraposición, el enfoque tradcional de la autenticación en red de las tarjetas inteligentes se ha basado en: dependencia del terminal para las labores de autenticación remota, en una solución de solicitante dividido y de claras consecuencias negativas para la seguridad; o en el potencial acceso a los servicios de autenticación en capa 3 o superiores (previsible en la tecnología de *network smart cards*), lo que conduciría a pilas de protocolos *aligeradas* y que podrían derivar en problemas de seguridad e incluso de interoperabilidad. Un enfoque en este sentido, que podría ser denominado *enfoque basado en red/transporte* o incluso *en aplicación*, requeriría, al mismo tiempo, de mejores condiciones en el interfaz de comunicación en tiempo real de la tarjeta inteligente, para soportar las características de dicho tráfico; este requerimiento se haría especialmente sensible en el caso de tarjetas sin contactos.

Como ventaja adicional del nuevo *Marco de Autenticación de Autenticación para Tarjetas Inteligentes en Red*, ha de resaltarse la versatilidad ante el cambio que se está produciendo en la tecnología de las tarjetas, ya que permitiría su aplicación tanto a las actuales tarjetas ISO 7816 como a las futuras *network smart cards*.

7.2. Trabajos Futuros

A lo largo del desarrollo de esta tesis se han identificado un conjunto de líneas de trabajo muy relacionadas con las componentes que se han tratado y que, aunque algunas de ellas se han incorporado como parte del mismo ampliando las perspectivas iniciales, han quedado finalmente al margen de los objetivos a cumplir. La continuidad del esas líneas estimulan futuras tareas, para dar complemento al presente trabajo.

7.2.1. Validación futura del Marco de Autenticación

La validación del Marco de Autenticación presentado ante la migración hacia la *Network Smart Card*, queda pendiente ante la expectativa de la evolución definitiva que experimentará esta tecnología. La correlación con los protocolos en diferentes capas que finalmente se vayan integrando en la tarjeta inteligente en red, dará cabida a una interesante inercia de continuidad, en la que cabe la validación del Marco de Autenticación aquí propuesto. Como se ha mencionado, dicho marco no sólo no debería ser un obstáculo para la incorporación de otros protocolos, sino que por el contrario podría favorecerla.

7.2.2. Arquitectura de autenticación y servicios

En este sentido, podría considerarse la provisión de otros servicios a la tarjeta. Los mecanismos aquí estudiados se han centrado en todo momento a los referidos a la autenticación de dispositivos en sí misma, sin atender a los servicios posteriores que pudieran brindarse. La interacción entre los servicios de autenticación remota para tarjetas inteligentes y esos otros servicios ofrecidos por el Emisor u otras entidades, identifican una interesante línea de trabajo futuro.

Respecto a la localización del servidor de autenticación, SAUT, podrían considerarse redes pertenecientes o no al mismo dominio que el terminal. La discusión sobre si este servidor de autenticación es el mismo que soporta la autenticación de la tarjeta inteligente corresponde a cada escenario particular; en cualquier caso, ambas opciones son posibles y en gran medida responderá a las correspondientes políticas de *roaming*, así como de los acuerdos de servicios y legales en el plano administrativo. Los modelos de negocio derivados de los acuerdos necesarios entre las partes involucradas (proveedor de redes locales inalámbricas (públicas), operador de telefonía móvil y entidades finales) podría también recaer en el estudio futuro.

En un enfoque opcional al presentado, el punto de acceso PA podría mantener su funcionalidad de *autenticador*, convirtiéndose el EU en un elemento netamente de *relay*. En dicho caso, este *autenticador* podría ser el mismo que diera servicio de autenticación a los EUs registrados en una determinada red local de acceso; unas políticas de seguridad adecuadas deben considerarse, en tanto que, podrían pertenecer a distintos dominios – tarjeta inteligente y EU, y dispondrían de distintos servidores de autenticación SAUT.

7.2.3. Aplicación a escenarios de Pago Electrónico

La creación formalizada de un Método EAP de tipo EMV (EAP-EMV, EAP-type=EMV), en principio ha quedado fuera del alcance de este trabajo y se pospone para trabajos futuros. No obstante el protocolo aplicado sobre el escenario de autenticación *on-li*ne con tarjetas inteligentes EMV, y que se ha descrito en detalle en esta tesis, facilita en gran medida la definición de tal método. Por completar esta idea, baste decir que la generación de ARQC en la tarjeta y ARPC en el Emisor, constituirían en sí mismo el núcleo de este Método EAP. La fijación de los valores de los *Types* y la concreción del contenido de los mensajes EMV, podrían formar parte de un proceso de estandarización como borrador de Internet (*Internet-Draft*), siendo objeto de trabajos posteriores.

7.2.4. Aplicación a otros escenarios

La aplicación a otros escenarios de nuestro de Marco de Autenticación para Tarjetas Inteligentes en Red es inmediata a la vista de las ventajas que supone en términos de interoperabilidad y facilidad de implementación. En definitiva, su aplicación podría considerarse para todos aquellos escenarios que implicaran un servicio de autenticación

remota. Por ejemplo, en el ámbito del DNI o pasaporte electrónico resultaría de relevante interés en caso de que se produjera un servicio de autenticación on-line. Así, podría tomarse significativa ventaja de nuestra propuesta en aquellos entornos en los que, por las características del servicio eventual o permanente, fuese necesario un esquema centralizado de autenticación.

7.2.5. Ampliación a otros dispositivos

Ha de observarse que el Marco de Autenticación propuesto puede ser igualmente válido para otros dispositivos distintos a las tarjetas inteligentes. En tal caso, nuestro Modelo de Multiplexación de EAP para éstas no sería aplicable y en su lugar podría no ser necesario un componente análogo, dependiendo de las características del dispositivo que se introdujera en el esquema. En esta misma línea, podría considerarse el anidamiento en el Modelo Extendido de Autenticación, cuyo análisis de seguridad podría llevarse a cabo según se indicó en el epígrafe 3.5.2.

Bibliografía

Bibliografía

[3DS01] 3D –Secure Functional Specification, Chip Card Specification v1.0, Visa Corp., August 2001.

[3G-23060] 3GPP TS 23.060 V7.2.0, General Packet Radio Service (GPRS);Service description; Stage 2, September 2006.

[3G-23234] 3GPP TS 23.234 v7.3.0: 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description, September, 2006.

[3G-31116] 3GPP TS 31.116 V6.8.0 Remote APDU Structure for (U)SIM Toolkit applications, June 2005.

[3G-33234] 3GPP TS 33.234 v7.2.0; 3GPP System to Wireless Local Area Network (WLAN) Interworking Security System, September 2006.

[3G-43020] 3GPP TS 43.020 V6.4.0, Security related network functions, June 2006.

[802.11] IEEE Standard for Information Technology, 802.11, 1999 Edition (R2003) Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2003.

[802.11i] IEEE Standard for Information technology, 802.11i-2004 Amendment to IEEE Std 802.11i/D7.0: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security, 2004

[802.1X] IEEE Standard for Information technology, 802.1X IEEE-2004. Standard for Local and metropolitan area networks. Port-based network Access Control, December 2004

[Aba93] Abadi, M., Burrows, M., Kaufman, C. and Lampson, B., Authentication and delegation with smart-cards, Science of Computer Programming, Vol. 21, Issue 2, pp. 93-113, 1993.

[Abd97] Abdul-Rahman, A.and Hailes, S., A distributed trust model. In Proceedings of the Workshop on New Security Paradigms, NSPW '97, Langdale, Cumbria, U.K., September 1997.

[Abo03] Aboba, B., Calhoum, P., RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), IETF RFC 3579, September 2003.

[Abo04] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H., Extensible Authentication Protocol (EAP), IETF RFC 3748, Standards Track, June 2004.

[Abo99] Aboba, B., Simon, D.: PPP EAP TLS Authentication Protocol, IETF RFC 2716, October 1999.

[Ahm03] Ahmavaara, K.., Haverinen, H., Pichna, R., Interworking architecture between 3GPP and WLAN systems, IEEE Communications Magazine, Vol.41, No.11, pp. 74- 81, November 2003.

[Ali05] Ali, A., Lu, K. and Montgomery, M., Network Smart Card: A New Paradigm of Secure On-line Transactions, In Proc. of Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20th International Conference on Information Security (SEC 2005), May 30 - June 1, 2005, Chiba, Japan.

[And96] Anderson, R. and Kuhn, M., Tamper resistance -- A cautionary note", In Proc. of Usenix Workshop Electronic Commerce, pp. 1-11, 1996.

[And97] Anderson, R. and Kuhn, M., Low-Cost Attacks on Tamper-Resistant Devices, Security Protocol Workshop' 97, LNCS 1361, pp. 125-136, April 1997.

[And98] Anderson, R. J., Biham, E., Knudsen, L. R., Serpent and Smartcards, In Proc. of International Conference on Smart Card Research and Applications, CARDIS '98, Louvain-la-Neuve, Belgium, September 1998, LNCS 1820, pp. 246-253, 1998

[Ark06] Arkko, J. and Haverinen, H., Extensible Authentication Protocol Method for 3rd Generation Authenticationand Key Agreement (EAP-AKA), IETF RFC 4187, January 2006.

[Bar04] Bargh, M.S., Hulsebosch, R.J., Eertink, E.H., Prasad, A., Wang, H. and Schoo, P., Fast authentication methods for handovers between IEEE 802.11 wireless LANs. In Proceedings of the 2nd ACM international Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, WMASH '04, Philadelphia, PA, USA, October 2004.

[Bet88] Beth, T., Efficient Zero-Knowledge Identification Scheme for Smart Cards, LNCS 330, pp. 77- , January 1988.

[Bic03] Bicakci, K., Baykal, N., One-Time Passwords: Security Analysis Using BAN Logic and Integrating with Smartcard Authentication, LNCS 2869, pp. 794 - 801, October 2003.

[Bir04] Biryukov, A., Lano, J., Preneel, B., Cryptanalysis of the Alleged SecurID Hash Function, LNCS 3006, pp. 130 - 144, January 2004.

[Bor01] Borst, J., Preneel, B. and Rijmen, V., Cryptography on smart cards, Computer Networks, Volume 36, Issue 4, pp. 423-435, July 2001.

[Bos95] Bosselaers, A. and Preneel, B., Integrity Primitives for Secure Information Systems, Final Report of the RACE Integrity Primitives Evaluation (RIPE, RACE R1040), LNCS 1007, Springer-Verlag, 1995.

[BRA01] IST Project Brain. Broadband Radio Access for IP based Networks (IST-1999-10050), 2001.

[Bra89] Braden, R., Requirements for Internet Hosts –Communication Layers, IETF RFC 1122, October 1989.

[Bri01] Brier, E., Handschuh, H., Tymen, C., Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware, LNCS 2162, pp. 16-27, January 2001.

[BTv2] Bluetooth Specification Version 2.0, Vol. 0, Promoter Members of Bluetooth SIG, Inc., June , 2004.

[Buc03] Bucci, M., Germani, L., Luzzi, R., Trifiletti, A., Varanonuovo, M., A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC, IEEE Transactions on Computers, Volume 52 , Issue 4, pp. 403 - 409, April 2003.

[Bur90] Burrows, M., Abadi, M., Needham, R., A Logic of Authentication, ACM Transactions on Computer Systems, Vol. 8, No. 1, pp.18-36, 1990.

[Cha01] Chan, A. T., Tse, F., Cao, J., and Leong, H. V., Distributed Object Programming Environment for Smart Card Application Development. In Proc. of the Third international Symposium on Distributed Objects and Applications (September 17 - 20, 2001), IEEE Computer Society, 2001.

[Cha02] Chan, A., Tse, F., Cao, J. and Leong, H.V., Enabling Distributed Corba Access to Smart Card Applications. IEEE Internet Computing, Vol. 6, No. 3, pp. 27-36, May-June 2002.

[Cha04] Chang,Y., Chang, C., and Kuo, J. 2004. A secure one-time password authentication scheme using smart cards without limiting login times. SIGOPS Oper. Syst. Rev. 38, 4 , pp. 80-90, October 2004.

[Cha05] Chan, A.T.S, Mobile cookies management on a smart card, Communications of the ACM, Vol. 48, No. 11, pp. 38 - 43, 2005.

[ChC01] Chan, A.T.S, Cao, J., Chan, H.and Young, G.H., A web-enabled framework for smart card applications in health services. Communications of the ACM, Vol. 4, No.9, pp. 76-82, 2001.

[Che00] Chen, Z.: Java Card Technology for Smart Cards: Architecture and Programmers´s Guide. The Java Series. Addison Wesley Professional, June 2000.

[Chi02] Chien, H. Y., Jan J.K. and Tseng Y. M., An efficient and practical solution to remote authentication: smart card, Computers & Security, Vol. 21, No. 4, pp. 372-375, 2002.

[CMT] Comisión del Mercado de las Telecomunicaciones, España, http://www.cmt.es

[Con03] Contini, S. and Yin, Y.L., Improved Cryptanalysis of SecurID, Cryptology ePrint Archive: Report 2003/205

[Des87] Desmedt, Y., Quisquater J-J., Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference between DES and RSA?) , LNCS 263, p. 111, January 1987

[Dev03] Deville, D., Galland, A., Grimaud, G., Jean, S., Assessing the Future of Smart Card Operating Systems. In Proc. of the International Conference on Research in Smart Cards, e-SMART 2003, Nice, France, 2003.

[Don01] Donsez, D., Jean, S. And Lecomte, S., Turning Multi-Applications Smart Card Services Available from Anywhere at Anytime: a SOAP/MOM approach in the context of Java Cards. In Proc. of Smart Card Programming and Security Conference. e-Smart 2001, Cannes, France, 2001.

[ElG85] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. on Information Theory, Vol. 31, No. 4, pp. 469-472, July 1985.

[EMV] EMV, Integrated Circuit Card, Specifications for Payment Systems: http://www.emvco.com

[EMV04-2] EMV, Integrated Circuit Card, Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.1, June 2004

[EMV04-3] EMV, Integrated Circuit Card, Specifications for Payment Systems, Book 3, Application Specification,Version 4.1, May 2004

[Ero05] Eronen, P., Hiller, T., Zorn, G., Diameter Extensible Authentication Protocol (EAP) Application, IETF RFC 4072, August 2005.

[EVO04] IST Project EVOLUTE, seamlEss multimedia serVices Over alL IP-based infrastrUcTurEs, (IST-2001-32449) , 2004

[Fan05] Fan, .C-I., Chan, Y.-C and Zhang Z.-K., Robust remote authentication scheme with smart cards, Computers & Security, Vol. 24, Issue 8, pp. 619-628, 2005.

[Fia87] Fiat, A., Shamir, A., How to prove yourself: practical solutions to identification and signature problems, Advances in Cryptology – Proceedings of Crypto '86, LNCS 263, pp. 186–194, 1987.

[FIPS 140-2] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, December 03, 2002

[FIPS 180-2] FIPS PUB 180-2 , Secure Hash Standard, August 01, 2002.

[Fis84] Fischer, M.J., Micali, S., Rackoff, C., A secure protocol for the oblivious transfer, Eurocrypt'84 pero publicado en Journal Cryptology 9 (3), pp. 191–195, 1996.

[Fri06] Friedrich, E. and Seidel, U., The introduction of the German e-passport, Journal of Documents & Identity, Issue 16, 2006.

[Fun06] Funk, P., Blake-Wilson, S., EAP Tunneled TLS Authentication Protocol Version 1, (EAP-TTLSv1), Internet-Draft , <draft-funk-eap-ttls-v1-01.txt>, March 2006

[Gol89] Goldwasser, S., Micali, S. and Rackoff, C., The knowledge complexity of interactive proof systems. SIAM J. Comput. 18, pp. 186–208, 1989.

[Gri03] Grimaud, G., Vandewalle, J.J.: Introducing Research Issues for Next Generation Java-based Smart Card Platforms. In Proc. of Smart Objects Conference, SOC'03, Grenoble, France, 2003.

[Gui01] Guillou, L.C., Ugon, M. and Quisquater, J-J., Cryptographic authentication protocols for smart cards, Computer Networks, Vol. 36, Issue 4, pp. 437-451, 2001.

[Gui89] Guillou, L.C. and Quisquater, J-J., A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory, Advances in Cryptology – Proceedings of Eurocrypt '88, LNCS 330, pp. 123–128, 1989.

[Gui90] L. Guillou, J-J. Quisquater, A paradoxical identity-based signature scheme resulting from zero-knowledge, Advances in Cryptology – Proceedings of Crypto '88, LNCS 403, pp. 216–231, 1990.

[Gut00] Guthery, S, Kehr, R. and Posegga, J., How to Turn a GSM SIM into a Web Server. Projecting Mobile Trust onto World Wide Web. In Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS '00, Bristol, United Kingdom, 2000.

[Hal95] Haller, N., The S/KEY One-Time Password System, IETF RFC 1760, February 1995.

[Hal98] Haller, N., Metz, C., Nesser, P., Straw, M., A One-Time Password System, IETF RFC 2289, February 1998.

[Han98] Handschuh, H., Paillier, P.: Smart Card Crypto-Coprocessors for Public-Key-Cryptography. In Proc. of Smart Card Research and Applications, CARDIS '98, Louvain-la-Neuve, Belgium, 1998.

[Hav06] Haverinen, H. and Salowey, J: Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM), IETF RFC 4186, January 2006.

[Hsu04] Hsu, C.L., Security of Chien et al's remote user authentication scheme using smart card, Computer Standards and Interfaces, Vol. 26, Issue 3, pp. 167-169, 2004.

[Hwa00] Hwang, M. S. and Li, L. H., A new remote user authentication scheme using smart cards, IEEE Trans. Consumer Electronic, Vol. 46, No. 1, pp. 28-30, 2000.

[ISO 11568-2] Banking – Key management (retail) – Part 2: Key management techniques for symmetric ciphers, ISO 11568-2:1994

[ISO 8583-1] Financial transaction card originated messages -- Interchange message specifications -- Part 1: Messages, data elements and code values, ISO 8583-1:2003.

[ISO/IEC 10116] Information technology – Security techniques – Modes of operation for an n-bit block cipher, ISO/IEC 10116

[ISO/IEC 10118-3] Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions, ISO/IEC 10118-3

[ISO/IEC 10536] Identification cards -- Contactless integrated circuit(s) cards -- Close-coupled cards -- Part 1: Physical characteristics, ISO/IEC 10536-1:2000

[ISO/IEC 14443] Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Parts 1-3, ISO/IEC 14443

[ISO/IEC 15693] Identification cards -- Contactless integrated circuit(s) cards -- Vicinity cards -- Parts 1-3, ISO/IEC 15693:2000

[ISO/IEC 9796-2] Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, ISO/IEC 9796-2:2002

[ISO/IEC 9797-1] Information technology – Security techniques – Message Authentication Codes - Part 1:Mechanisms using a block cipher, ISO 11568-2:1994

[ISO7816] Identification cards -- Integrated circuit(s) cards with contacts -- Parts 1 - 15, ISO/IEC 7816:2005

[ISO7816-12] Identification cards - Integrated circuit cards -- Part 12: Cards with contacts -- USB electrical interface and operating procedures, ISO/IEC 7816-12:2005

[Ito00] Itoi, N., Fukuzawa, T. and Honeyman, P., Secure Internet Smartcards. Java on Smart Cards: Programming and Security, First International Workshop, JavaCard 2000, LNCS 2041, Cannes, France, September 14, 2000.

[Ito99] Itoi, N. and Honeyman, P., Smartcard Integration with Kerberos V5, USENIX Workshop on Smartcard, Chicago, Illinois, USA, 1999.

[JCD] http://java.sun.com/products/javacard/dev_kit.html

[Jua04] Juang, W.-S., Efficient password authenticated key agreement using smart cards, Computers & Security, Vol. 23, Issue 2, pp. 167-173, 2004.

[Jua99] Juang, W.-S., Lei, C.-L. and Chang, C.-Y., Anonymous channel and authentication in wireless communications, Computer Communications, Vol. 22, Issues 15-16, pp. 1502-1511, 1999.

[Kam04] Kambourakis, G., Rouskas, A., Kormentzas, G., Gritzalis, S., Advanced SSL/TLS-based authentication for secure WLAN-3G interworking. IEE Proceedings Communications, Vol. 151, Issue 5, pp. 501 – 506, October 2004.

[Kam05] Kambourakis, G., Rouskas, A., Gritzalis, S., Geniatakis, D., Support of Subscribers Certificates in a Hybrid WLAN-3G Environment, Computer Networks, Vol. 50, Issue 11, pp. 1843-1859, August 2006.

[Kle06] Kleef, F.van, Biometrics in the Dutch passport, Journal of Documents & Identity, Issue 16, 2006.

[Koc99] Kocher, P., Jaffe, J. and Jun, B., Differential power analysis, In Proc.of Advances in Cryptology (CRYPTO '99), pp. 388-397, August 1999.

[Koi03] Koien, G.M., Haslestad, T., Security aspects of 3G-WLAN interworking, IEEE Communications Magazine, Vol. 41, Issue 11, pp. 82 - 88, November 2003.

[Köm99] Kömmerling, O., Kuhm, M.G., Design principles for Tamper-Resistant Smartcard Processors. In Proc. of USENIX 1st Workshop on Smartcard Technology, Chicago, USA, 1999.

[Kra92] Krawjewski, M., Concept for a Smart Card Kerberos. In National Computer Security Conference, No. 15, pp. 76-83. National Institute of Science and Technology, US Deptartment of Commerce, 1992.

[KuC04] Ku, W. C., and Chen, S. M., Weaknesses and improvements of an efficient password based user authentication scheme using smart cards, IEEE Trans. Consumer Electronic, Vol. 50, No. 1, pp. 204 –207, 2004.

[Lam81] Lamport, L., Password authentication with insecure communication, Communications of the ACM, Vol. 24, No. 11, pp. 770-772, 1981.

[Lea95] Leach, J., Dynamic authentication for smartcards, Computers & Security, Vol. 14, Issue 5, pp. 385-389, 1995.

[Lee02] Lee, C.C., Hwang, M. S., Yang, W. P., A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review, Vol. 36, Issue 4, pp. 23-29, 2002.

[Lee04] Lee, S.W., Kim, H.S. and Yoo, K.Y., Improved efficient remote user authentication scheme using smart cards, IEEE Transactions on Communications, Vol. 50, pp. 565–567, 2004.

[Leu06] Leu, J-S. Lai, R-H., Lin, H-I. Shih, W.K., Running cellular/PWLAN services: practical considerations for cellular/PWLAN architecture supporting interoperator roaming, IEEE Communications Magazine, Vol.44, No.2, pp. 73- 84, February 2006.

[Lia06] Liao, I-E., Lee, C.C. and Hwang, M.S., A password authentication scheme over insecure networks, Journal of Computer and System Sciences, Vol. 72, Issue 4, pp. 727-740, Volume 72, June 2006.

[LIPMAN] NURIT 8000 by Lipman. Wireless POS features: http://www.lipmanusa.com/site/sites/USA/lipman.asp?pi=775&doc_id=1848, visited on October 2006.

[Liu04] Liu, Z., Joy, T. and Thompson, R., A Dynamic Trust Model for Mobile Ad Hoc Networks, In the 10th IEEE International Workshop on Future Trends in Distributed Computing Systems, FTDCS '04, Suzhou, China, May 2004.

[LuK04a] Lu, H.K. New Advances in Smart Card Communications, International Conference on Computing, Communications And Control technologies (CCCT), Austin, TX, USA, August 14-17, 2004.

[LuK04b] Lu H.K. and Ali A., Prevent On-line Identity Theft - Using Network Smart Cards for Secure On-line Transactions. In Proc of 7th International Conference on Information Security, ISC '04, Palo Alto, CA, USA, September 27-29, 2004.

[LuK06] Lu, H.K., Multi-stage Packet Filtering in Network Smart Cards, In Proc. of 6th IFIP Smart Card Research and Advanced Application Conference, CARDIS '06, Tarragona, Spain, LNCS 3928, pp. 192-205, 2006.

[Man00] Manchala, D.W., E-Commerce Trust Metrics and Models, IEEE Internet Computing, Vol. 4, No. 2, pp. 36-44, 2000.

[Man05] Mantin, I., A Practical Attack on the Fixed RC4 in the WEP Mode, Advances in Cryptology - ASIACRYPT 2005, LNCS 3785, pp. 395-411, 2005.

[Mar05] Marquez, F.G., Rodriguez, M.G., Valladares, T.R., de Miguel, T., Galindo, L.A., Interworking of IP multimedia core networks between 3GPP and WLAN, IEEE Wireless Communications, [see also IEEE Personal Communications], Vol.12, No.3, pp. 58- 65, June 2005.

[Mel06] Melnikov, A., Zeilenga, K., Simple Authentication and Security Layer (SASL), IETF RFC 4422, June 2006.

[Mic90] Micali, K., Shamir, A., An improvement of the Fiat–Shamir identification and signature scheme, Advances in Cryptology – Proceedings of Crypto '88, LNCS. 403, pp. 244–247, 1990.

[Mit89] Mitchell, C., Limitation of a challenge- response entity authentication, Electronic Letters, Vol. 25, No.17, pp. 1195- 1196, 1989.

[Mon04] Montgomery, M., Ali, A. and Lu H.K., Secure Network Card. Implementation of a Standard Network Stack in a Smart Card, In Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS '04, Toulouse, France, Kluwer Academic Publishers, August 23-26, 2004.

[Moo02] Moore, S., Anderson, R., Cunningham, P., Mullins, R., Taylor, G., Improving smart card security using self-timed circuits, In Proc. of 8th International Symposium on Asynchronous Circuits and Systems, pp. 211- 218, April 2002.

[Nee78] Needham, R.M., Schroeder, M.D., Using encryption for authentication in large networks of computers, Communications of the ACM, Vol. 21, Issue 12, pp. 993-999, 1978.

[Neu94] Neuman, C., and T. Ts'o, Kerberos: An Authentication Service for Computer Networks, IEEE Communications, Vol. 32, No.9, 1994.

[NIST 800-63] Burr, W.E., Dodson, D.F. and Polk, W.T., Electronic Authentication Guideline, National Institute of Standards and Technology, NIST-SP-800-63, v1.0.2 , April 2006

[Noo00] Noore, A., Highly robust biometric smart card design, IEEE Transactions on Consumer Electronics, Vol.46, No.4, pp.1059-1063, November 2000.

[Nys00] Nystrom, M., The SecurID(r) SASL Mechanism , IETF RFC 2808, April 2000.

[Osw06] Oswald, E., Mangard, S., Herbst, C. and Tillich, S., Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers, LNCS 3860, pp. 192 - 207, December 2006.

[Pha06] Phan R. C-W., Cryptanalysis of two password-based authentication schemes using smart cards, Computers & Security, Vol. 25, Issue 1, pp. 52-54, 2006.

[PKCS#11] PKCS #11 v2.20: Cryptographic Token Interface Standard, RSA Laboratories, June 2004.

[Qui01] Quisquater, J.J. and Samyde, D., ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In Proc. of the International Conference on Research in Smart Cards: Smart Card Programming and Security, LNCS 2140, pp. 200-210, 2001.

[Qui97] Quisquater, J.J.: The adolescence of Smart Cards. Future Generation Computer Systems, Vol. 13, Issue 1, pp. 3-7, June 1997.

[Raj05] Rajavelsamy, R., Jeedigunta, V., Holur, B., Choudhary, M., Song, O., Performance evaluation of VoIP over 3G-WLAN interworking system, IEEE Wireless Communications and Networking Conference, Vol.4, No.13-17, pp. 2312- 2317, March 2005.

[Ree00] Rees, J. and Honeyman, P., Webcard: a Java Card web server. In Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS '00, Bristol, U.K., 2000.

[RES03] IST Project RESET, Roadmap for European Research on Smartcard related Technologies, IST-2001-39046: Final Roadmap v.5, May 2003.

[Rig00] Rigney, C., Willens, S., Rubens, A., Simpson, W., Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, June 2000.

[Rou05] Rouine, M. and Murphy, C., The New Irish Passport - New passport, new system, new processes, Journal of Documents & Identity, Issue 14, 2005.

[Sal02] Salkintzis, A., Fors, C. and Pazhyannur, R. S., WLAN-GPRS Integrationfor Next Generation Mobile Data Networks, IEEE Wireless Communications, Vol. 9, No. 5, pp. 112-124, October 2002.

[Sal03] Salgarelli, L., Buddhikot, M., Garay, J., Patel, S., Miller, S., Efficient authentication and key distribution in wireless IP networks. IEEE Wireless Communications, Vol. 10, Issue 6, pp. 52 – 61, December 2003.

[Sal04] Salkintzis, A.K., Interworking techniques and architectures for WLAN/3G integration toward 4G mobile data networks, IEEE Wireless Communications, Vol. 11, Issue. 3, pp. 50 – 61, June 2004.

[San03] Sanchez-Reillo, R., Mengibar-Pozo, L., Sanchez-Avila, C., Microprocessor smart cards with fingerprint user authentication, IEEE Aerospace and Electronic Systems Magazine, Vol.18, No.3, pp. 22- 24, March 2003.

[SAT06] 3GPP TS 31.111 V7.5.0, Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface, September 2006.

[Sch98] Schneier, B. and Whiting, D., Twofish on Smart Cards, In Proc. of International Conference on Smart Card Research and Applications, CARDIS '98, Louvain-la-Neuve, Belgium, LNCS 1820, , pp. 14-16, September 1998.

[SCP04] ETSI Technical Specification 102.310 v6.0.0: Smart Cards; Extensible Authentication Protocol support in the UICC, December 2004.

[Sha00] Shamir, A., Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies, LNCS 1965, pp. 71- , Jan 2000.

[Sha84] Shamir, A., Identity-based cryptosystems and signature schemes, Advances in Cryptology; Crypto'84, LNCS 196, pp. 47-53, 1984.

[Sha95] Shamir, A., Memory Efficient Variants of Public-Key Schemes for Smart Card Applications, LNCS 950, pp: 445- , May 1995.

[She03] Shen, J. J., Lin, C.W. and Hwang, A modified remote user authentication scheme using smart cards, IEEE Trans. Consumer Electronic, Vol. 49, No. 2, pp. 414-416, 2003.

[Shie06] Shieh, W.-G. and Wang, J.-M., Efficient remote mutual authentication and key agreement, Computers & Security, Vol. 25, Issue 1, pp. 72-77, 2006.

[ShM06] Shin, M., Ma, J., Mishra, A., Arbaugh, W.A., Wireless network security and interworking, Proceedings of the IEEE , Vol.94, No.2, pp. 455- 466, February 2006.

[Sid05] Siddiqui, F., Zeadally, S., Yaprak, E., Design Architectures for 3G and IEEE 802.11 WLAN Integration, LNCS 3421, pp. 1047 - 1054, January 2005.

[Sim94] Simpson, W., The Point-to-Point Protocol (PPP), IETF RFC 1661, Standard Track, July 1994.

[Sko03] Skorobogatov, S.P., Anderson, R.J., Optical Fault Induction Attacks, LNCS 2523, pp. 2-12, January 2003.

[Son05] Song, W., Jiang, H., Zhuang, W., Shen, X., Resource management for QoS support in cellular/WLAN interworking, IEEE Network , Vol.19, No.5, pp. 12- 18, Sept.-Oct. 2005.

[Sta05] Stanley, D., Walker, J., Aboba, B., Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, IETF RFC 4017, March 2005.

[Stu04] Stubblefield, A., Ioannidis, J., and Rubin, A. D. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Trans. Inf. Syst. Secur. 7(2), pp. 319-332, May 2004.

[SUI02] IST Project SUITED. Multi-segment System for broadband Ubiquitous access to Inernet services and Demonstrator (IST 1999-10469), 2002.

[SUN06] Java Card™ Platform, Version 2.2.2, Sun Microsystems, Inc., Santa Clara, California 95054, U.S.A, 2006.

[Sur03] Surtees, A., McCann, S., Hepworth, E., Riegel, M., Combining W-ISP and cellular interworking models for WLAN, 4th International Conference on 3G Mobile Communication Technologies, 2003, pp. 259-263, June 2003.

[THALES] Artema GSM BlueTooth by Thales e-transactions. Wireless POS features: http://www.thales-e-transactions.com/solutions/mobile/gsm_bt.php, visited on October 2006.

[Tor05] Torres, J., Izquierdo, A., Ribagorda, A. Alcaide, A.: Secure electronic Payments in heterogeneous networking: new authentication protocols approach, LNCS 3482, pp.729-738, 2005.

[Tor06a] Torres, J., Izquierdo, A., Sierra, J.M. and Ribagorda, A., Towards self-authenticable smart cards, Computer Communications, Volume 29, Issue 15, pp. 2781-2787, Volume 29, Issue 15, 5 September 2006.

[Tor06b] Torres, J., Izquierdo, A., Sierra, J.M. and Ribagorda, A., A realistic approach on password-based remote mutual authentication schemes with smart cards, Pendiente de Publicación

[Tri01] Trichina, E., Bucci, M., De Seta, D., Luzzi, R., Supplemental Cryptographic Hardware for Smart Cards, IEEE Micro, Nov-Dec 2001, pp. 26-35.

[Uri00] Urien, P., Internet card, a smart card as a true Internet node. Computer Communications, Vol. 23, Issue 17, pp. 1655-1666, 2000.

[Uri04] Urien, P., Badra, M., Dandjinou, M., EAP-TLS Smartcards, from Dream to Reality. In Proc. of 4th IEEE Workshop on Applications and Services in Wireless Networks, Boston, USA, August 2004.

[Uri06] Urien, P., Pujolle, G., EAP Smart Card Protocol, IETF Internet Draft <draft-urien-eap-smartcard-type-10>, August 2006.

[USB00] Universal Serial Bus Specification, Revision 2.0, USB Implementers Forum, Inc. (USB-IF), December 21, 2000.

[USB05] Universal Serial Bus Communications Class Subclass Specification for Ethernet Emulation Model Devices, Revision 1.0, USB Implementers Forum, Inc. (USB-IF), February 2, 2005.

[Vol05] Vollbrecht, J., Eronen, P., Petroni, N., Ohba, Y., State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator, IETF RFC 4137, August 2005.

[WI-FI] Wi-Fi Alliance, http://www.wi-fi.org/

[WIN01] IST Project Wine. Wireless Internet Networks. (IST-1999-10028), 2001.

[Xio03] Xiong, L., Liu, L., A reputation-based trust model for peer-to-peer e-commerce communities, IEEE International Conference on E-Commerce, 2003. CEC 2003, pp. 275- 284, June 2003.

[Xiu05] Daoxi Xiu and Zhaoyu Liu, "A Dynamic Trust Model for Pervasive Computing Environments", the Fourth Annual Security Conference, Las Vegas, NV, March 30-31, 2005

[Yoo05] Yoon, Y.E., Ryu, K. and Yoo, K.Y., An improvement of Hwang–Lee–Tang's simple remote user authentication scheme, Computers & Security, Vol. 24, Issue 1, pp. 50–56, 2005.

[Yoo06] Yoon, E-U., Yoo, K-Y., One-Time Password Authentication Scheme Using Smart Cards Providing User Anonymity, LNCS 3984, pp. 303 - 311, May 2006.

[Zha06] Zhao, Y., Lin, C., Yin, H., Security Authentication of 3G-WLAN Interworking, 20th International Conference on Advanced Information Networking and Applications, AINA '06, Vol.2, pp. 429- 436, April 2006.