RESUMEN DEL PROYECTO FIN DE CARRERA

Desarrollo de un nuevo sistema de acceso y comunicación para los terminales de pago con los centros de autorización bancarios a través de pasarelas IP/X.25 utilizando ADSL y GPRS.

Autor: ***D. Roberto Javier López Sastre***
Director: ***D. Manuel Utrilla Manso***
Departamento de Teoría de la Señal y Comunicaciones
Escuela Politécnica Superior

XXVI CONVOCATORIA DE PREMIOS
"Ingenieros de Telecomunicación"

I. Introducción

En el Proyecto fin de Carrera titulado, “*Desarrollo de un nuevo sistema de acceso y comunicación para los terminales de pago con los centros de autorización bancarios a través de pasarelas IP/X.25 utilizando ADSL y GPRS*”, presentamos una nueva filosofía de servicio para el escenario de los medios de pago en España. Nuestra propuesta se fundamenta en conseguir que los medios de pago se modernicen y comiencen a utilizar las redes de banda ancha y GPRS, y en un cambio de toda la arquitectura de red que garantice la total integración de los actuales modelos de TPV's (Terminal Punto de Venta) que las entidades financieras tienen instalados en los distintos comercios.

A continuación describiremos el porqué de esta investigación, los objetivos perseguidos, las fases de desarrollo y las conclusiones obtenidas.

A. ORIGEN DE LA INVESTIGACIÓN

Actualmente en España hay instalados más de 900.000 TPV's que utilizan la RTC (Red Telefónica Conmutada) como medio físico para la transmisión de las transacciones electrónicas. Esta situación conlleva que por cada transacción originada desde el TPV se desencadena una llamada telefónica para poder establecer una comunicación con el Centro Autorizador de una Entidad Financiera. Estas llamadas son costeadas por los usuarios de los TPV's y vienen a durar una media de 20 segundos, contando la fase de establecimiento y de marcado. En la figura 1 podemos ver representada la arquitectura de red que sostiene este servicio.

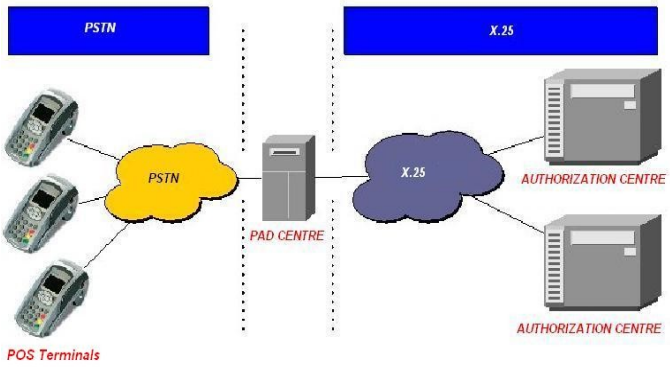

Fig. 1: Escenario actual de los medios de pago en España

El TPV, también llamado POS (Point Of Sale), no se comunica directamente con el centro autorizador vía RTC. Las entidades financieras han colocado todos sus centros de autorización y host's bancarios en la red X.25 IBERPAC creada por la compañía Telefónica España. Por tanto, la transacción originada en un TPV debe llegar hasta la red X.25. Disponer en cada punto de venta de un acceso a la red X.25 sería impensable, debido al elevado coste, de hecho, esta situación solo se aplica a grandes superficies comerciales que manejan un gran volumen de transacciones electrónicas. Bajo esta tesitura, resulta evidente que necesitamos de un elemento de red que nos

permita concentrar todas las llamadas telefónicas y nos de acceso a la red X.25, en definitiva, que funcione como una pasarela (*gateway*) entre estas dos redes. Este elemento fue llamado centro PAD (Packet Assembler/Disassembler) y ha sido implantado por Telefónica España. Simplemente marcando el 090 desde cualquier terminal telefónico accederemos al centro PAD más cercano que nos dará acceso a la red X.25 IBERPAC. Hoy en día hay más compañías que disponen de estos centros para dar acceso a los TPV's, pero sin duda ha sido Telefónica España la que comenzó con esta filosofía de servicio.

Este servicio lleva funcionando en nuestro país durante más de 30 años y no es nuestra intención establecer una crítica destructiva, pero sí identificar las carencias y problemas que ha presentado:

- Cada transacción implica el tener que desencadenar una llamada telefónica.
- Imposibilidad de utilizar la línea telefónica para realizar operaciones de forma concurrente.
- Cada llamada lleva un tiempo de marcado y de establecimiento que ralentizan el servicio.
- Las comunicaciones desde el TPV hasta el centro PAD son vía módem (desde 2400 Bps hasta 9600 Bps).
- Los centros PAD pueden estar congestionados y la llamada será rechazada.

Podríamos decir que el escenario de los medios de pago en España ha estado dormido. Son muchos los avances en servicios y elementos de red que podrían permitir una mejora en el sistema que está actualmente en explotación. Si tenemos en cuenta la creciente demanda de tarjetas de crédito y débito, así como la revolución que VISA y MasterCard van a introducir en el mercado con el nuevo estándar de tarjetas EMV (Europay MasterCard Visa) a partir del año 2008, entonces encontraremos que se hace necesaria una mejora en el servicio actual. Desde este proyecto vamos a presentar una nueva filosofía de servicio para los medios de pago que permita solucionar todos estos problemas, que abarate el servicio, lo haga más rápido y le dote de mayores mecanismos de seguridad.

B. OBJETIVOS DE LA INVESTIGACIÓN

Una vez descrito el escenario actual, que supone nuestro punto de partida, podremos entender los objetivos que perseguimos, y podríamos resumirlos en los siguientes puntos:

- El nuevo servicio va a utilizar las tecnologías ADSL y GPRS como medio físico para el acceso a la red X.25.
- La red X.25 no va a ser sustituida pues las entidades financieras no están dispuestas a modificar sus estructuras de conectividad para el Host, además, aunque obsoleta, la red X.25 ha demostrado que funciona muy bien para tráfico de tipo transaccional. Existen alternativas que montan el nivel de red X.25 sobre TCP, es lo que se conoce como XOT (X.25 Over TCP). Estos equipos permiten transmitir todo el "nivel de red" a través de una red TCP/IP y no tener que cambiar los interfaces de conexión de los Host's.
- Necesitamos de un nuevo elemento de red que permita acceder desde ADSL o GPRS hasta la red X.25. Este elemento es una pasarela TCP/X.25 y sustituirá al centro PAD

que veíamos en la Figura 1.

- Para incrementar la seguridad del servicio, añadiremos una serie de mecanismos de seguridad a la pasarela.
- Queremos dotar de movilidad al servicio. Para ello, necesitaremos de una tecnología como GPRS que nos garantiza una cobertura total y un ancho de banda suficiente para un tráfico de tipo transaccional.

Desde este proyecto proponemos dos filosofías de servicio. Una basada en ADSL y otra en GPRS. La de GPRS la podemos subdividir en dos: servicio sobre GPRS sin intranet o servicio sobre GPRS con intranet.

La Figura 2 muestra el esquema de servicio basado en ADSL, y la Figura 3 nos muestra el servicio basado en GPRS con y sin intranet.

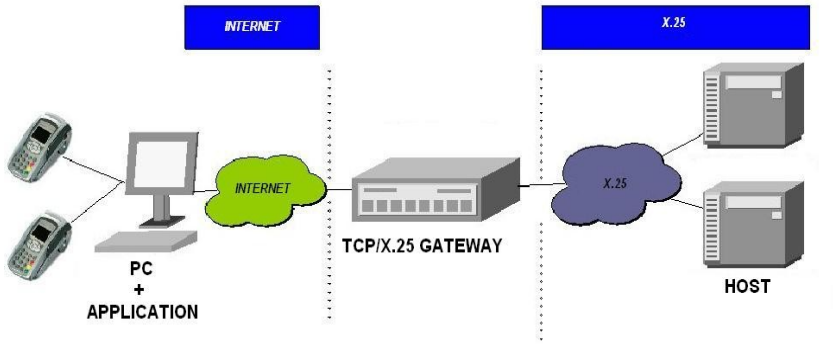

Fig.2 Escenario basado en ADSL

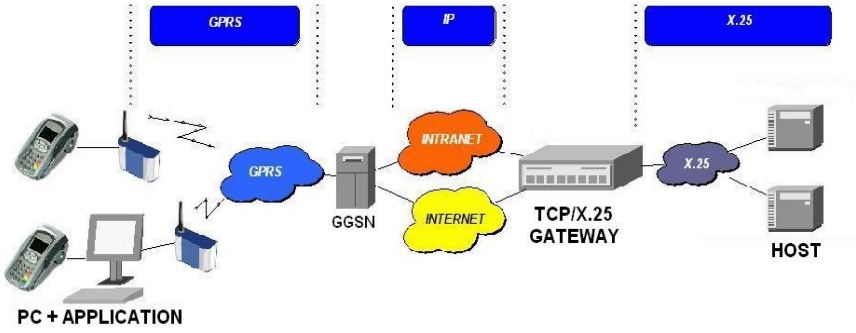

Fig.3 Escenario basado en GPRS

Antes de explicar cada uno de los escenarios presentados, creemos que es relevante explicar como podemos conectar los TPV's a estos sistemas. Nuestro proyecto pretende ser un proyecto de integración, en el que no sólo los nuevos modelos de TPV's que están saliendo al mercado (que llevan integrado un stack TCP-IP, puertos de conexión Ethernet, módulos radio GPRS, etc.), puedan acceder a nuestro servicio, sino que cualquier modelo de TPV instalado hoy en día pueda beneficiarse de esta nueva filosofía de servicio.

Para conseguir esto necesitamos de un PC con una aplicación desarrollada adecuadamente. Esta aplicación deberá comunicarse con el TPV, vía un puerto RS-232 que todos los modelos de TPV disponen, y con la pasarela. La aplicación la hemos desarrollado para este proyecto y permite integrar todos los modelos de TPV del mercado en estos nuevos servicios.

Al igual que en todos los TPV's existe un puerto para línea telefónica, existe también un puerto RS-232 por el que se les carga el software de la entidad bancaria que los ha comprado. Todos ellos pueden ser configurados para que emitan las transacciones a través de un puerto u otro. Nosotros vamos a utilizar este puerto COM para que el TPV se comunique con la aplicación que corre en el PC y que dialogará con la pasarela para hacer llegar las transacciones originadas en el TPV hasta el centro autorizador bancario. Lo que proponemos es un nuevo sistema de acceso, un nuevo servicio, pero además hemos desarrollado la aplicación que permite integrar todo el parque actual de TPV's, por ello se trata de un proyecto no sólo de desarrollo, sino también de integración.

Con los escenarios de servicios propuestos pretendemos cubrir todas las posibles situaciones del cliente. Sin duda, el servicio que mayor complejidad de red presenta es el basado en GPRS con intranet. A día de hoy cualquier operador de telefonía móvil ofrece este servicio de conectividad, lo que nos permitirá disponer de una red privada desde el operador hasta nuestra pasarela. En este escenario se hace necesario incluir, como se detalla en el Proyecto Fin de Carrera, un elemento que controle el acceso a nuestra red, que es llamado RADIUS. Añadiendo este último elemento de red tendríamos completa la arquitectura del servicio.

C. DESARROLLO DEL SISTEMA

A continuación vamos a explicar los interfaces del sistema así como las características de seguridad implementadas.

C.1 Interfaces del sistema y protocolos implementados.

En el nuevo modelo de servicio que proponemos existen dos interfaces claramente diferenciables. El interfaz I1, entre PC y TPV, y el interfaz I2 entre PC y Pasarela. Las características de cada uno de ellos vienen impuestas por los elementos que relacionan y, sobre todo en el interfaz I2, por las entidades financieras y emisoras de tarjetas. Es evidente, que para el interfaz I2 nos hemos acogido a las recomendaciones realizadas desde VISA, y por algunas entidades financieras, para garantizar la seguridad de las transacciones que viajan por Internet o por una intranet.

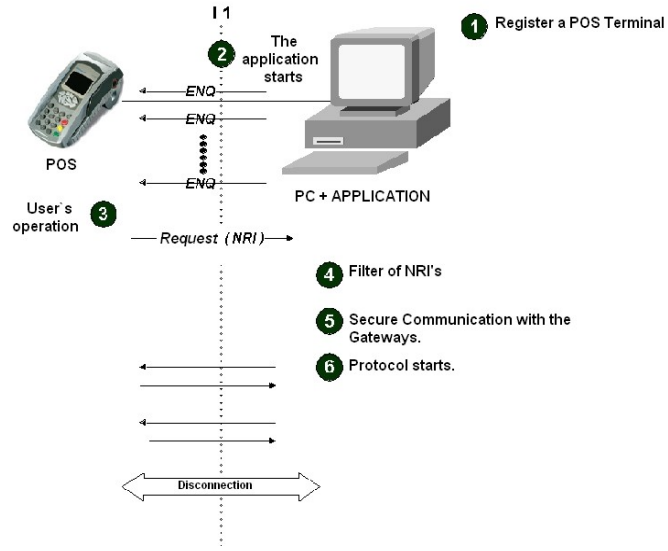

Fig. 4 Protocolo interfaz I1

El proyecto se ha desarrollado centrándonos en cada uno de los interfaces y en su intercomunicación. El

interfaz I2 se ha diseñado para que los TPV's de nueva generación puedan acceder directamente a la pasarela, sin pasar por la aplicación.

Los protocolos que se han desarrollado para el interfaz I1 e I2 son los que se presentan en las figuras 4 y 5 respectivamente. Para una explicación más detallada de los protocolos implementados (tamaño de los mensajes, cabeceras, timeouts, ...), remitimos al lector al Proyecto fin de Carrera.

El protocolo del interfaz I1 se ajusta al protocolo que existe entre centro PAD y TPV en el escenario actual. Sobre el interfaz I2 se ha realizado la mayor parte del trabajo garantizando: que los requisitos de seguridad que impone VISA se cumplen, y que se trata de un sistema al que puedan conectarse todos los modelos de TPV's.

C2. Mecanismos de seguridad.

Sin duda alguna al tratarse de un escenario como el de los medios de pago, la seguridad ha sido al capítulo más importante de la investigación, junto con el diseño de la arquitectura de red.

Los protocolos de seguridad implementados son los exigidos por las entidades financieras españolas para la transmisión a través de redes no privadas. La seguridad del sistema se basa en la combinación de: algoritmos de cifrado RC4, algoritmos de firma Hash MD5, y de procedimientos de carga segura de claves. Obtenemos asíun servicio de transporte de datos seguro pues se cubren los requisitos de: confidencialidad, integridad, autenticidad, no repudio y no replica. La Figura 6 muestra las fases del protocolo donde se generan los desafíos y las semillas dinámicas. La pasarela y nuestra aplicación disponen de una clave base, cargada siguiendo uno de los procedimientos de carga segura de claves definido por las entidades financieras, que se va a utilizar en la primera fase de negociación y desafío para cifrar los datos. Con esta clave y un algoritmo aleatorio generaremos las claves dinámicas con las que vamos a cifrar las comunicaciones. El procedimiento que se muestra en la Figura 6 arranca cuando la aplicación c ontacta con la pasarela.

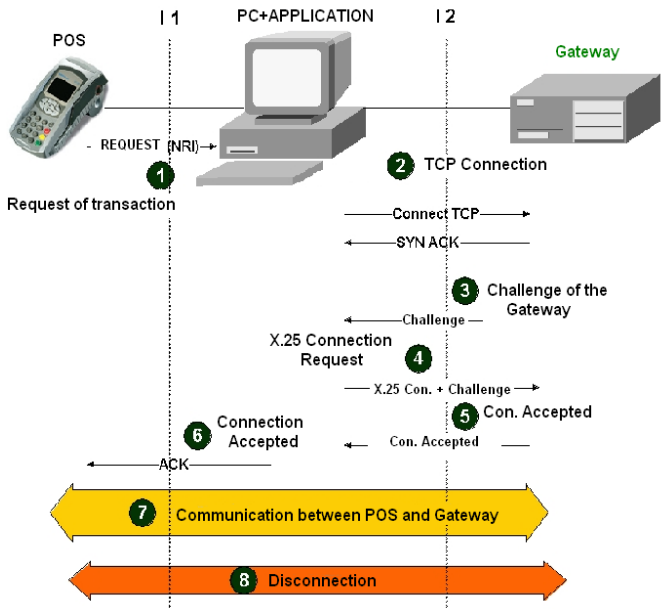

Fig. 5 Protocolo interfaz I2.

D. CONCLUSIONES

Son muchos los fabricantes de TPV's que hoy en día fabrican sus modelos con todo lo necesario para garantizar la conectividad a este nuevo modelo de servicios. Desde este proyecto ofrecemos un servicio que permite integrar los medios de pago tradicionales en las redes IP. Las ventajas que ofrecen estos servicios son muy significativas:

- Utilización de ADSL y GPRS en lugar de la línea telefónica.
- Posibilidad de realizar transacciones de forma simultánea.
- Abaratamiento del coste de las transacciones.
- Aumento de la velocidad.
- Aumento de la seguridad del sistema.
- Eliminación de los tiempos y costes de establecimiento.
- Posibilidad de disfrutar de movilidad en el escenario GPRS.
- Debido a la rapidez de estos servicios, el tiempo medio de transacción es de 5 segundos, todas las transacciones son autorizadas *on-line*, lo que supone el fin del fraude *off-line* que existe hoy en día.

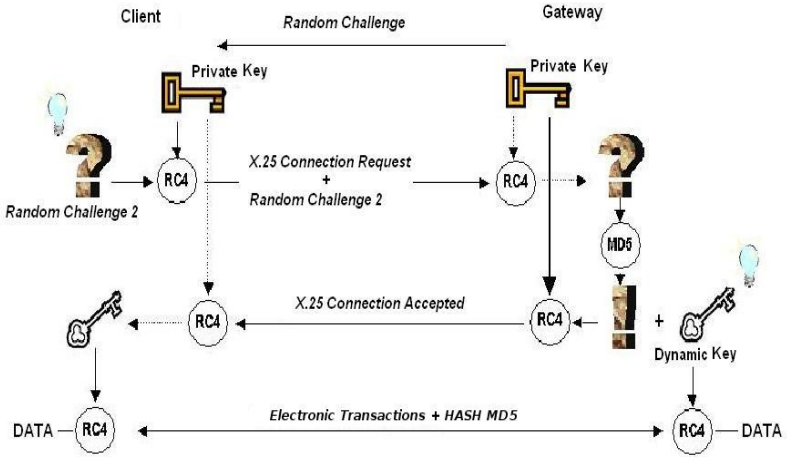

Fig. 6 Mecanismos de seguridad.

El proyecto desarrollado presenta un nuevo servicio para los medios de pago. Los servicios descritos se han implantado en escenarios reales y con entidades financieras que a día de hoy los tienen en funcionamiento. Las soluciones propuestas nos llevan a la integración definitiva de los medios de pago en las tecnologías de banda ancha y tecnologías móviles. El proyecto realizado presenta la implementación de un nuevo servicio para los medios de pago basado en redes IP. Es sin duda un proyecto de integración, pues permite que los nuevos modelos de TPV's y los tradicionales coexistan y compartan la misma arquitectura de red. Con este proyecto hemos realizado algunos trabajos que han sido publicados en diferentes congresos científicos nacionales e internacionales, y cuyas referencias bibliográficas se indican en el anexo de esta documentación. Sin duda alguna, las futuras líneas de investigación irán dirigidas a garantizar las exigencias de seguridad que vendrán impuestas en el nuevo estándar de tarjetas EMV, defendido por VISA y MasterCard.

II. Originalidad

Desde este proyecto proponemos una nueva filosofía servicio basada en una arquitectura de red que integra redes de banda ancha y de movilidad. El escenario actual sobre el que se sustentan los TPV's es sin duda un escenario obsoleto, en el que apenas se había introducido modificaciones en su arquitectura de red para modernizarlo. Los escenario implementados en este trabajo de investigación integran en el servicio las conexiones ADSL y GPRS.

El ADSL va a suponer la capacidad de realizar un gran volumen de transacciones desde un único cliente. Ya no será necesario, por tanto, el tener que realizar una instalación de una conexión X.25 para un gran cliente. Ahora, simplemente con una conexión ADSL y un PC con nuestra aplicación, seremos capaces de conectar todos los TPV's que queramos con el centro autorizador, y de forma *on-line.* Actualmente en el mercado existen algunos sistemas semejantes al nuestro, pero no utilizan un PC para canalizar las transacciones y además el servicio sólo se ofrece a través de conexiones ADSL de determinadas compañías telefónicas. Además, nosotros proponemos que los TPV's se concentren en un PC que nos podría servir para tareas de gestión y contabilidad. La conexión desde el PC hasta la pasarela la podemos hacer con el operador que deseemos, gracias a todos los mecanismo de seguridad que hemos implementado para el diálogo entre pasarela y aplicación.

La red GPRS va a dotar a los TPV's de la posibilidad de movilidad, se trata de acercar los medios de pago electrónicos a escenarios donde antes no se podía: empresas de transportes, repartidores, taxis, restaurantes, etc. Nuestro sistema fue instalado en varios taxis y resultó ser un éxito. Bien es cierto que para el escenario GPRS se desarrolló un sistema que permitía conectar el TPV directamente al módem GPRS, sin necesidad de PC. Pero el escenario GPRS no está pensado sólo para clientes que necesiten movilidad. Hay pequeños comercios que no necesitan de ADSL, y para ellos una conexión a través de GPRS va a resultar mucho más económica, como veremos en el apartado III de este resumen, si el volumen de transacciones no es muy elevado. Luego el escenario GPRS, aunque en él no se disfrute de la movilidad, resulta quizás mucho más atractivo y económico a la mayoría de los clientes. Se decidió trabajar con GPRS y no con UMTS por tres razones:

1. La red GPRS nos daba un cobertura nacional completa.
2. La naturaleza del tráfico a generar es puramente transaccional, y el ancho de banda de GPRS nos permitía realizar una transacción a gran velocidad.
3. UMTS se presentaba como una tecnología muy cara y poco desarrollada en el momento de desarrollar nuestro proyecto.

Como he dicho antes, nuestra intención no es realizar una crítica destructiva del actual sistema, pues ha demostrado su correcto funcionamiento durante más de 30 años. Lo que pretendemos es una renovación que ofrezca a los usuarios un servicio más rápido y seguro. La demanda de velocidad es una realidad. Cada vez son más las tarjetas de crédito y débito, y las colas a la hora de pagar cada vez son mayores. Una alternativa para solucionar estos problemas es trabajar en *off-line*. Esto se ha venido haciendo en muchas gasolineras con gran cantidad de clientes en horas puntas, y quizás el caso más conocido es el de los peajes de las autopistas. El *off-line* traía consigo una gran cantidad de fraude que ha preocupado a las entidades financieras y a los emisores de tarjetas. Con los escenario propuestos podemos tener transacciones autorizadas en 3 segundos sobre

el esquema ADSL. Si nos ponemos en una zona de peajes, donde todas las máquinas están conectadas a un PC con nuestra aplicación y con una conexión ADSL a nuestra pasarela, podríamos autorizar todas las transacciones de forma concurrente y *on-line*. Luego, como vemos, los nuevos servicios para los medios de pago sobre IP suponen el fin del *off-line* y de su fraude asociado, todo se puede autorizar *on-line* pues ya no es tan lento el sistema.

III. Resultados

Los resultados obtenidos que vamos a presentar se han conseguido con el escenario ADSL sobre una conexión de 1Mb y con el escenario GPRS sobre una conexión sin intranet y con intranet.

Para el escenario ADSL las transacciones quedan autorizadas en un tiempo medio de 3 segundos, y para el escenario GPRS, con y sin intranet, la duración media de una transacción es de 5 segundos. Estos tiempos han sido obtenidos realizando medidas en diferentes situaciones de carga de red, y simplemente vienen a dar una medida aproximada del gran incremento de velocidad que ha experimentado el servicio de cara al usuario.

La siguiente gráfica muestra el análisis económico de cara al usuario.

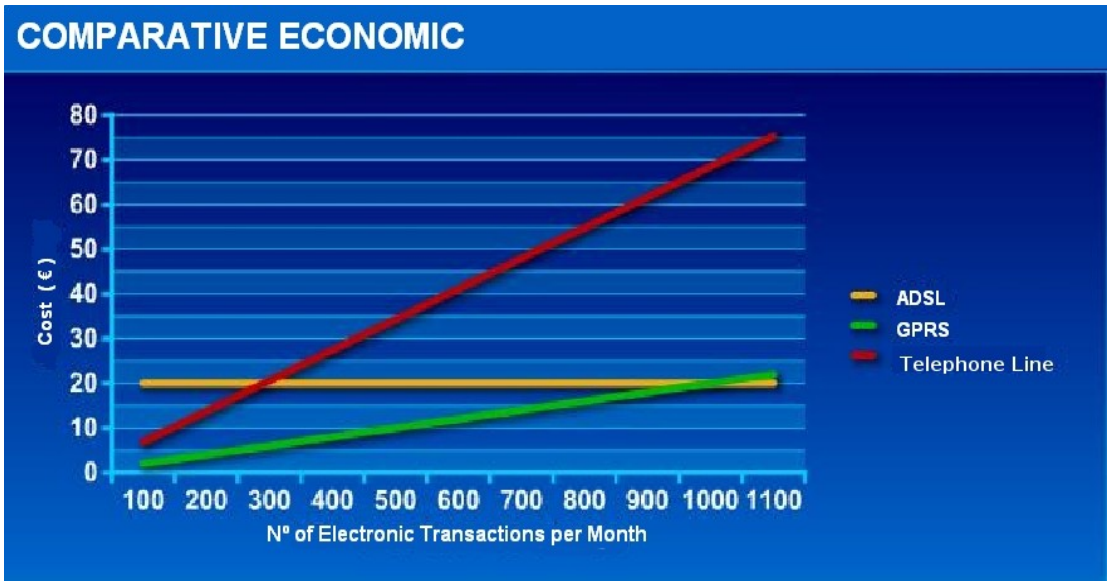

Fig. 7 Comparativa Económica.

Como podemos observar, la solución basada en la línea telefónica, que representa el escenario actual, es la más cara debido a su crecimiento lineal. Al usuario final le resulta mucho más económico el sistema basado en GPRS siempre que el número de transacciones que realice al mes sea inferior a 1000, si no es así, la solución sobre ADSL es la más económica.

IV. Aplicabilidad

La aplicabilidad del sistema queda patente en el hecho de que han sido barias entidades financieras las que se han interesado e instalado el sistema. El proyecto fue desarrollado en colaboración con las empresas: SAGEM España (http://www.sagem.com/nso/es/spa/) y Grupo de Negocios COPEL (http://www.grupo-copel.com/neuron.htm).

Cómo hemos resaltado, el objetivo que perseguimos es un nuevo servicio que permite la integración de los modelos actuales de TPV's en los nuevos servicios, y esta filosofía trae consigo un aumento en la aplicabilidad del sistema. Las entidades financieras ya no tiene que adquirir nuevos modelos de TPV's , pues los antiguos sirven para modernizar el sistema, y esto supone un gran ahorro en la inversión a realizar. Remitimos al lector al Proyecto fin de Carrera si desea analizar la propuesta económica que allí hacemos para una implantación real.

A. Anexo

Publicaciones en congresos

R.J. López Sastre, "***Nuevo Servicio de Comunicaciones para los medios de pago basados en pasarelas IP/.X25****", XX Simposium Nacional de la URSI, Gandía (Valencia), 14-16 Septiembre de 2005.*

R.J. López Sastre, F.J. López Herrero, S. Lafuente Arroyo, A. Vázquez Reina, "***Electronic Funds Transfer Service over GPRS and Secure TCP/X.25 Gateways***", *WSEAS AIKED 2006, Alcalá de Henares (Madrid), 15-17 February de 2006.*

R.J. López Sastre, S. Maldonado Bascón, F.J. López Herrero, "***New Electronic Funds Transfer Services over IP****", IEEE Melecon 2006, Benalmádena (Málaga), 16-19 Mayo de 2006.*