Proceedings of the 5th WSEAS Int. Conf. on Artificial Intelligence, Knowledge Engineering and Data Bases, Madrid, Spain, February 15-17, 2006 (pp153-158)

Electronic Funds Transfer Service over GPRS and Secure TCP/X.25 Gateways.

F.J. LÓPEZ HERRERO
Company EQUIN S.A.
Dpt. of Research and Technology
C/Primavera, 14 28805 Torrejón de Ardoz
Spain
http://www.equinsa.es

R.J. LÓPEZ SASTRE, S. LAFUENTE ARROYO
A. VÁZQUEZ REINA
University of Alcalá de Henares
Dpt. of Signal Theory and Communications
Edificio Politécnico, 28871 Alcalá de Henares
Spain
http://www2.uah.es/teose/

Abstract: This paper shows a complete description of a new EFT (Electronic Funds Transfer) service over IP for the traditional payment terminals. This new EFT service carries all the electronic transactions, generated from the POS (Point Of Sale) Terminals to the Authorization Centres (Host) through an IP network with secure TCP/X.25 gateways. At first, the system establishes a secure connection with the TCP/X.25 gateway, then the electronic transaction is ciphered and transmitted to the Host. This work presents a solution based on the transmission technology GPRS (General Packet Radio Service). These new service improves the current solutions because it is cheaper, faster and more secure. The security of the system has been the most important chapter in this investigation work, and this paper describes all the security algorithms implemented and it presents the results obtained.

Key–Words: EFT, POS terminal, banking, electronic transaction, GPRS, X.25, TCP, gateway, RC4, MD5.

1 Introduction

Nowadays, in Spain there are installed 900.000 POS (Point Of Sale) Terminals which use the PSTN (Public Switched Telephone Network) as their way of transmission. POS Terminals communicate with their Authorization Centre (Host) to make the electronic transactions. These centres are connected in Spain to a X.25 network called IBERPAC. In this kind of stage a POS Terminal has to access to this X.25 network for making transactions. This access is not made through an X.25 access point for every POS, it is done through the PAD (Packet Assembler/Disassembler) Centre, which is the element that works as a gateway, it takes the traffic originated from the POS, over a communication via modem, and converts it in X.25 traffic which is sent to the Host. Figure 1 shows all the parts of this system. From this described stage the communication between the POS and the Host is characterized by the following points:

- The PSTN network is the way of transmission from the POS to the PAD.
- A lot of time is lost in the dial and establishment step.
- Every electronic transaction originated in the POS involves a telephone call. In these terms, every electronic transaction has associated the establishment cost of the call too.
- The communications in the first interface are via modem, with speeds from 1200 Bps to 9600 Bps.

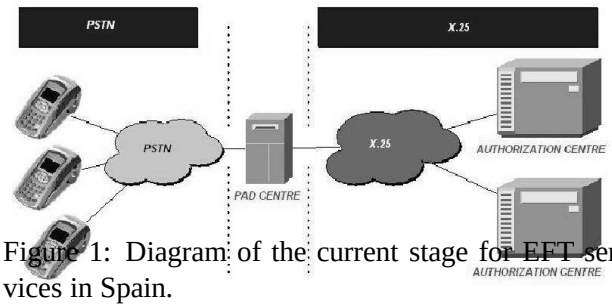

Figure 1: Diagram of the current stage for EFT services in Spain.

Figure 2 shows a graph which describes the exchange of messages and the steps of the protocol for the current EFT service. In this figure can be identified two different steps in the communication: a first one involves the POS and the PAD Centre, and the

second involves the Host too. A complete description of this protocol can be found in [1].

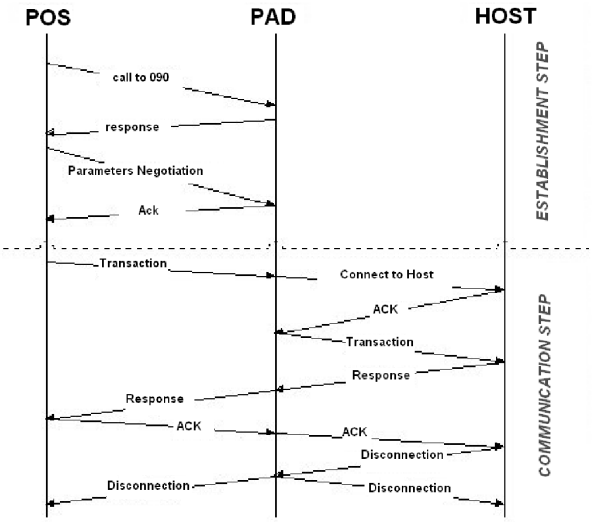

Figure 2: Communication Protocol between the POS terminals and the Host.

This paper proposes a new EFT service for the traditional POS terminals based in the transmission technology GPRS (General Packet Radio Service), which makes the communication faster and cheaper. This new service assumes that the X.25 network, in which are connected all the Host in Spain, can not be replaced. The new service needs an element which works as a PAD, it is the TCP/X.25 gateway. For this new service has been implemented some special TCP/X.25 gateways including security specifications described in section 4, which are accepted by all the banks and saving-banks. The figure 3 shows the new stage for the EFT service via GPRS.

The outline of this paper is as follows. In section 2 we introduce a complete description of the stage which supports the new service. Section 3 shows the communication protocols implemented, and in Section 4 is detailed all the security characteristics of the system. Results and conclusions comprise the final sections.

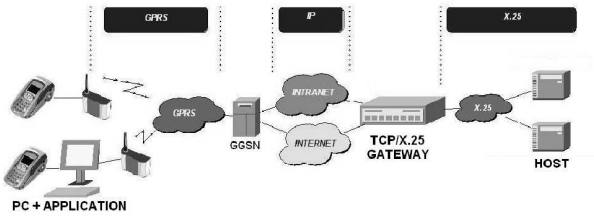

Figure 3: New stage for EFT service via GPRS.

2 New EFT service description.

The current EFT service has so many problems and costs described in section 1. The principal objective of this work is to implement a new service based in GPRS technology. Although it is so intuitive to think about the possibilities of mobility for the GPRS stage, we have to pay attention to other factors to decide that this stage is better than the current. For this work we have implemented the solution for the GPRS stage only, but these new EFT services over IP, which are described in [3], have the following common characteristics:

- The communication via modem over PSTN is substituted by new technologies of transmission.
- All the problems and inconveniences derived from the use of the telephone calls have been eliminated: dial and establishment step, busy line, slow transmissions, etc.
- Each transaction originated in these new services is cheaper than another one generated in the current system. This point is so important for the merchant.
- The speed of transmission is higher.
- The security of the system has been increased. With these new services it is possible to implement more security mechanisms than with the current system.
- These systems offer us voice calls and electronic transactions simultaneously.

2.1 Implementation via GPRS.

Figure 3 shows two possible implementations for the GPRS stage. A first one is based in a GPRS modem, which allows us to connect to the mobile operator, and a PC whith the application developed. The second scheme proposed is so different, we only need a POS Terminal and a GPRS modem, because we have designed a new application, for the modem, which allows the secure communication between the POS terminal and the Host. Figure 3 shows that it is possible that the transactions travel over Internet or over an intranet. In Figures 4 and 5 are defined all the interfaces and elements of the stages described. In these figures are represented only the solution based on PC, but as shows figure 3 it is possible to implement another stage only with a GPRS modem connected directly to a POS. In both cases the interfaces and network elements defined are the same.

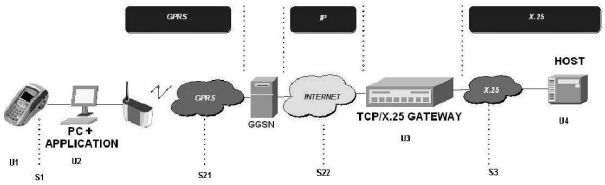

Figure 4: Interfaces and network elements of the service via GPRS without intranet.

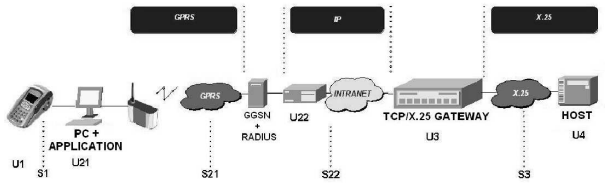

Figure 5: Interfaces and network elements of the service via GPRS with intranet.

The solution based on intranet needs that the mobile operator allows us to connect with him through a private network. Currently, mobile operators offer a lot of services of connectivity. The core network of an operator is showed in figure 6. This core supports connections of every authorized mobile client to Internet or to an intranet network. The element that connects every mobile terminal to other external networks is the GSSN (Gateway GPRS Support Node). All the packets travel through the GSSN, the SSSN (Serving GPRS Support Node) and the GPRS-IP network. The GPRS-IP network is so important for a mobile operator because if it wants to offer a big variety of services, it will need a correct dimensioned transport network which supports all of them. A mobile operator can offer a lot of services with this kind of network architecture, and for this investigation work we have used the intranet connection service.

In figure 5 appears a new element called RADIUS (Remote Authentication Dial-In User Service). The objective of this network element is to provide to the mobile terminal functions of: authentication and authorization. A RADIUS is needed because we have to control the access to a private network. Others solutions for access control can be used, but the mobile operators offer the RADIUS service as implemented solution. Every operator offers a lot of modalities of this service:

- Delegated or not delegated RADIUS: the mobile operator offers these two possibilities, the server in which the RADIUS service is installed can be managed for the mobile operator or for the client respectively.

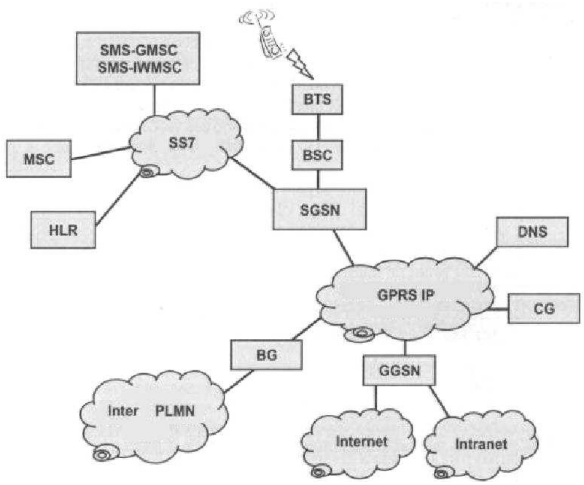

Figure 6: Core network of a mobile operator.

- Type of transmission technology: the mobile operator offers the intranet service over different technologies (Frame Relay, RDSI , ATM or IP).
- Characteristics of transmission: different rates and QoS (Quality Of Service).

In this kind of stage it is necessary to cipher the information in spite of using private networks, because the interface S21, in figure 5, is a radio network interface in which the information sent without a security algorithm could be listened.

3 Communication protocols.

We have defined two interfaces in our system: an interface I1 between the POS terminal and the PC or GPRS modem, and an interface I2 between the PC or GPRS modem and the TCP/X.25 gateway.

3.1 Interface I1-Protocol description.

The main objective of this project is to get that the traditional POS terminals can work in this new type of stage. The protocol implemented is an adaptation fully compatible with the current protocol which it is used by terminals. A complete description of this protocol can be found in [1]: formats, types and sizes of messages, timers used, all the possible communication errors , etc. Figure 7 shows the steps and messages that this protocol needs to make a electronic transaction.

The protocol has two main steps: at firs it is needed a call request, then the communication step starts. As figure 1 shows a PAD it is needed for making transactions. This element has disappeared in the new service, and in our application for the interface

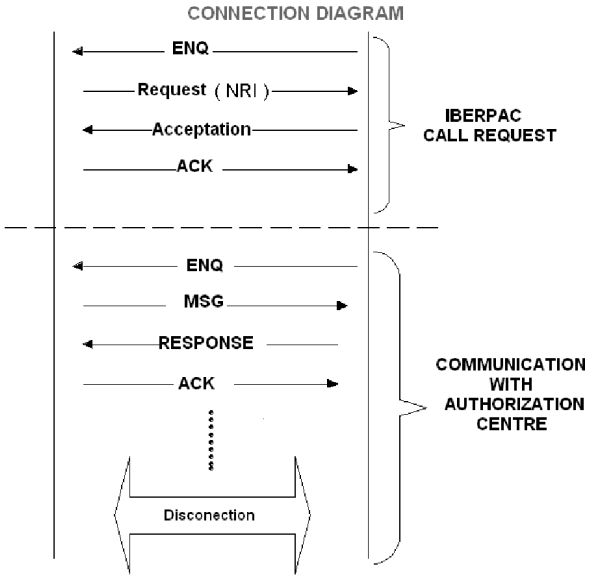

Figure 7: Messages of the protocol for the I1 interface.

I1, we have to simulate that we works as a PAD. The software implemented sends ENQs to the POS until an electronic transaction starts. From this point, the terminal sends the required NRI (Number of X.25 Network) to make the transaction. We have added to the protocol a NRI filter to increase the security of the system. If our filter identifies the NRI, then the application will start the second step showed in figure 7. In this step the POS terminals communicate with the Host, then it is needed a secure communication with the gateway. From this point, the protocol developed for the I1 interface follows the protocol implemented for the interface I2. Figure 8 shows the new protocol designed for the I1 interface. In this figure appears a PC based system, and the system based on GPRS modems only has the same structure and protocol implementation.

3.2 Interface I2-Protocol description.

This interface guarantees a secure communication with the gateway, and for the implementation of the protocol we have followed all the security specifications described in section 4. Figure 9 shows the steps of the protocol implemented: Connection, Data and Disconnection step. The first step starts when the protocol described for the interface I1 receives an authorized NRI. The application establishes a secure communication with the gateway during the connection step, in the next section are explained all the security characteristics used. Once the connection is completed, it starts the Data stage in which the POS and the Authorization Centre exchange messages. In

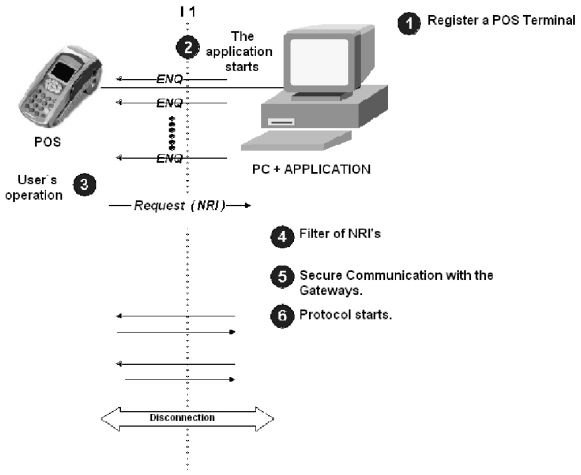

Figure 8: New protocol implemented for the interface I1.

the last step a disconnection is done. A detailed description that contains the format and the types of messages, and all of the characteristics developed, is not an objective of this paper, we only want to show that our software implementation follows the dialog scheme that appears in figure 10.

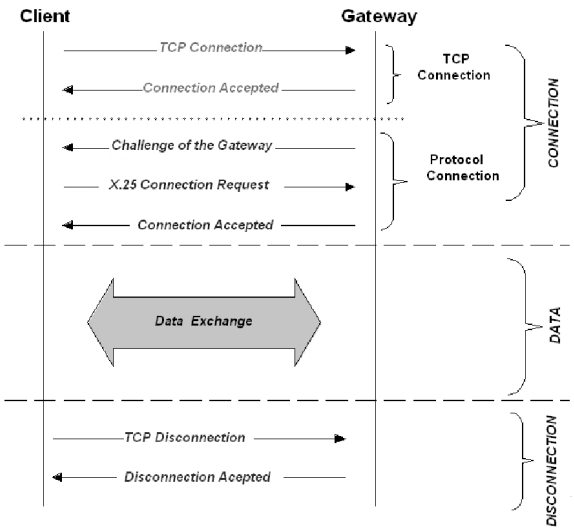

Figure 9: Description of the communication protocol with the TCP/X.25 gateway.

4 Security characteristics.

In the new EFT services investigation the main aspect is the security. The protocol developed follows to get a secure data transportation service, and to reach this objective it is necessary the next aspects:

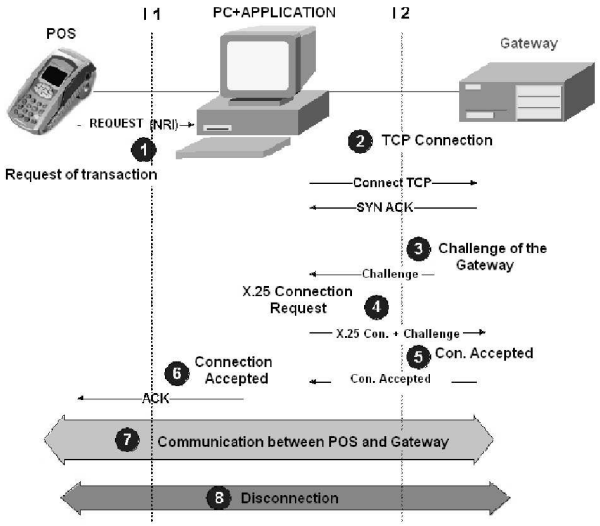

Figure 10: New protocol implemented for the interface I2.

- Confidentiality: it ensures that information is accessible only to those authorized to have access.
- Integrity: the condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- Authentication: it is the process by which a user attempts to confirm that the user from whom the second party has received some communication is, or is not, the claimed first party.
- Non-repudiation: non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively.

The security of our system is based in: a secure load of a private key, a stream cipher algorithm and a message digest procedure. The cipher algorithm used is the RC4 algorithm described in [4]-[6] and the message digest procedure employed is the HASH MD5 algorithm described in [7].

We have used a private key of 10 bytes to generate the random key which is used to cipher the messages. To make a secure service we have to guarantee that every client of our system has loaded the private key through a secure procedure. All of aspects related to secure procedures for loading keys in POS terminals are described in [2]. The mentioned procedures are imposed by banks and saving-banks. It is important to guarantee that the gateway can not be substituted to attack the private key in one client, to reach this objective our protocol introduces two challenges between the application and the gateway: one of them is generated from the gateway, and the client generates the other one. During the request connection step, the client and the gateway interchange a dynamic random key that will be used to cipher the messages of the session started. This procedure shows that the private key has been employed in the request stage only. For every new banking operation, and after the request stage, the client and the gateway work with a different dynamic key to cipher the messages. The gateway waits for a connection of a client, and when a connection is accepted the gateway generates a challenge based in a sequence of 64 bytes. From this point, the gateway waits for the X.25 connection request message of the client, which contains the response to the first challenge and a new challenge. If the response to the challenge is correct the algorithm will continue. The gateway needs to solve the challenge proposed from the client and it tries to establish a X.25 communication with the Host which is identified by the NRI. The response of the gateway contains: the solution to the challenge of the client and the new dynamic key of 10 bytes generated by a random algorithm. This last key is used to cipher all the messages of this session. In summary: only the swapped messages during the connection step are ciphered with the private key, and when the client receives the last message of the connection step it takes the new random key to cipher all the messages from this point. Figure 11 shows the procedure described.

Currently, the RC4 cipher algorithm is not recommended [8], but it is used in secure protocols as SSL (Secure Sockets Layer). We have implemented a secure procedure to use RC4, which is based on the security specifications of Tech Notes offered from the RSA Laboratories in [9]. The encryption keys used for RC4 are generated by hashing (using MD5), so that different sessions have unrelated keys. We do not re-key RC4 for each packet, but we use the RC4 algorithm state from the end of one packet to begin encryption with the next packet. To these characteristics it must be added that we use a secure load of private key and a double challenge procedure.

5 Results

These new stage proposed allows the users to increase the speed and decrease the cost of their electronic transactions. The tests realized, once the system was implemented and installed in real shops, show that in the current system the banking operations have an average time of 15 seconds, but now the average time is 5 seconds . In an economic comparative realized between the current system, the GPRS described in this paper, and an EFT service based on ADSL as de-

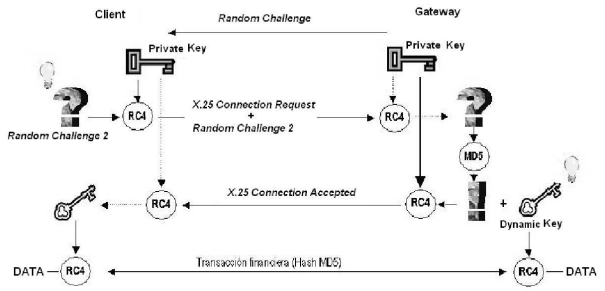

Figure 11: Security procedure.

scribed in [3], we obtained the figure 12, which shows that the cost of transmision of each electronic transaction has been reduced. If the shop realizes less than 1000 transactions every month (33 transactions every day) the GPRS service described is the best solution, instead of the EFT service via ADSL.

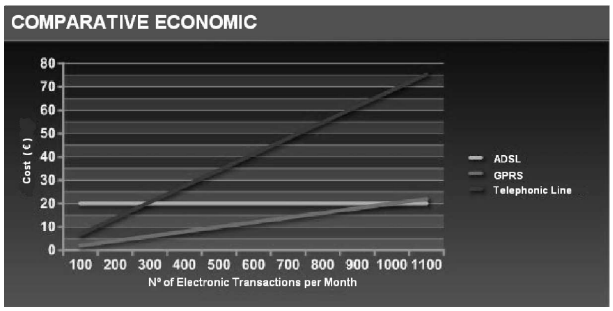

Figure 12: Economic comparative.

6 Conclusion

This paper makes a complete description of the new EFT service based on GPRS. The solution implemented is specific for the Spanish stage, but for other countries the system can be adapted changing the kind of gateway. The implementation and development of this service allows to adapt the traditional POS terminals to the GPRS technology. Currently, the manufacturers of POS terminals are including in their own equipments all needed hardware and software to integrate them in broad band technologies. They make POS terminals with: GPRS integrated, Ethernet ports, stack TCP/IP, ... The proposed service in this paper is fully compatible with these new models of POS terminals. So, this new stage allows the banks and saving-banks, which are the owners of the POSs, to avoid acquiring new models of them. Another important conclusion is that with the proposed service the off-line authorization does not make sense because in 5 seconds we have authorized transactions on-line. This is an important characteristic of this new service, because all the transactions are authorized on-line, and the off-line fraud disappears. There are so many places where the off-line authorization is needed because the on-line was too slow: toll gates in motorways, some petrol stations, etc.

Acknowledgements: We are sincerely grateful to the Department of Signal Theory and Communications of the UAH and EQUIN S.A. Company for their efficient help on this research.

References:

[1] SETSI, Real Decreto 81/1993 - Especificaciones técnicas de equipos de telecomunicaciones: X.28, X.32, DATÁFONO y HDLC/MNR, *BOE 41-1993*, 1993, pp. 4882–4913.

[2] F. Ayuso Gómez, Protocolo de acceso al servicio de pasarela IP/X.25 HYDRAMUX, *Alerta Comunicaciones*, Madrid 2003.

[3] R.J. LÓPEZ SASTRE, Nuevo servicio de comunicaciones para los medios de pago basado en pasarelas IP/X.25, *XX Simposio Nacional de la URSI*, Gandía, 2005.

[4] B. Schneier, *Applied Cryptography*, Ed. John Wiley & Sons, Second Edition, 1996, pp. 397–400.

[5] G. Pall,RFC 3078 Microsoft Point-to-Point Encryption (MPPE) protocol, *Microsoft Corporation*, http://www.ietf.org/rfc/rfc3078.txt, March 2001.

[6] K. Kaukonen and R. Thayer, A stream Cipher Encryption Algorithm ARC-FOUR, *IETF Draft - A Stream Cipher Encryption Algorithm Arcfour*, July 1999.

[7] R. Rivest,RFC 1321 The MD5 Message-Digest Algorithm, *MIT Laboratory for Computer Science and RSA Security*, http://www.ietf.org/rfc/rfc1321.txt, Inc. April 1992.

[8] S. Fluhrer,I. Mantin and A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, *Eighth Annual Workshop on Selected Areas in Cryptography*, August 2001.

[9] RSA Laboratories, Tech Notes: RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4, http://www.rsasecurity.com/rsalabs/node.asp?id=2009, 2001 .