New E-Payment Scenarios in an Extended Version of the Traditional Model

Mildrey Carbonell, Joaquin Torres, Antonio Izquierdo, and Diego Suarez

Universidad Carlos III de Madrid
Leganés (Madrid) Spain
{mcarbone,jtmarque,aizquier,dsuarez}@inf.uc3m.es

Abstract. Most of the security proposals in commerce scenarios have been based on a classical e-payment system definition. This definition basically represents a client who sends a payment order to obtain some goods/services from the merchant, which the intentions of the real money transaction carry on between his financial institutions. Nevertheless, these definitions are not sufficiently robust when new aspects appear in the electronic payment transaction. We can identify some of those new aspects (such as: smart card with network capabilities, business mediator with advantage services, handheld devices with constrained connectivity, and multiparty scenarios) that could subordinate the design of current and future commerce scenarios. In this paper we extended the traditional e-payment system definition, in order to include these new aspects. Additionally, we describe two new payment models, where such aspects are involved, and where the secure solution needs to consider new security requirements.

Keywords: E-payment system, secure payment protocol, multi-party scenarios, m-commerce, smart card.

1 Introduction

Since the appearance of e-commerce, significant work has been done trying to find a standard definition of e-payment system describing the principal involved entities and the flow of transactions in which these entities are involved.

Common to all of these approaches is the description of the e-payment system as the interaction of five principal entities: the business entities *client (C)* and *merchant (M)*, the financial entities *issuer (I)* and *acquirer (A)* and a *payment system provider (PSP)* as a secure entity which performs electronic payment transactions on behalf of the issuer and the acquirer on the Internet side and on behalf of client and merchant on the private banking network side.

However, this definition presents some limitations when describing the trends in current e-payment systems in which new aspects emerge, such as: business mediator, smart card, multiparty scenarios, and mobile devices, all of them creating new scenarios and circumstances which need new secure solution. The main goals of our research activity are to show the necessity to extend the e-payment system definition, and the necessity of design new security solution to payment process. For that, we present two

O. Gervasi et al. (Eds.): ICCSA 2008, Part II, LNCS 5073, pp. 514–525, 2008.

new payment models where many aspects are involved generating new flow of message and new security requirements.

Following, we start with the consideration of the traditional definition of e-payment system and the principal flow of his messages, in section 2. Afterwards, in section 3, we present the new aspects, that we will be considered, in the extended e-payment scheme. In section 4, the two new payment models, with their new flow of messages are described. And next, in section 5 we present a brief description of the new security requirements that appears due to these new aspects. The paper is concluded in section 6.

2 E-Payment Model

In many works, the payment model [1][2][3][4] is defined as the interactions between five principal entities (C, M, I, A, PSP) (fig. 1).

- **Client (*C*):** Entity who wants to purchase goods or services from a merchant.
- **Merchant (*M*):** Entity who delivers the goods/services upon receipt of payment.
- **Issuer (*I*):** The financial organization issuing the valid electronic payment instrument (for example, credit/debit card, account and others). He will transfer funds from the customer and acquirer bank.
- **Acquirer (*A*):** The financial organization of the merchant. He verifies the validity of the deposited payment and forwards it to the *PSP*, in order to inform the merchant.
- **Payment system provider (*PSP*):** IN [1] is defined as the entity which performs payment interactions on behalf of *I* and *A* on the Internet side, and on behalf of *C* and *M* on the private banking network side. He receives the request of payment authorization from the merchants and communicates with the issuer in order to obtain a response. He could communicate with the customer (depending on the electronic payment instrument) for obtaining some information (account, password, etc.). If the *payment authorization* request is successful, he sends to the merchant this information and withdraws from the merchant to inform the acquirer. The function of this entity may be implemented by a credit-card company (such as VISA with 3D Secure [2]), a mobile operator (such as mobipay [5]), a secure gateway (such as paypal [6], authorized.net [7]) or a bank.

The principal flow of messages in the payment process is:

1. *Payment ordering:* PO is the interaction between *C* and *M* , there, *C* requests to purchase goods or services from *M* sending the required information (amount of purchases, issuer identification by payment instruments, etc.) to carry out the payment
2. *Authorization request: AR* It is the interaction by which *M* requests a payment authorization from the customer's issuer and waits for a response. The payment authorization process is handled through a PSP with the following functionalities:
   a) *Off-line client authentication:* Where the PSP check the client information, received from merchants, without need an online client authentication. In that way, the merchant receives all the private information of client, forward it to the PSP and this one connects to the issuer bank.

b) *Online client authentication:* Where the PSP checks the client information, which is received from merchants, by means an online authentication mechanism (PIN, password, certificates, etc.). With this purpose, the PSP establishes an *authentication channel* with the client.

3. *Authorization response:* Where the PSP sends the response (successful or unsuccessful depending on issuer decision) of the authentication process to the merchants. If it is successful, the response it is sent to the acquirer, in order to conclude the purchase.
4. *Payment sending:* Finally, the payment process conclude with an interaction between *I* and *A,* with the goals of transferring the requested amount. Normally, this type of transaction is performed under a private banking network, once the acquirer has received a successful authorization response. This interaction ends when *A* forwards the payment receipt to *M* through a PSP.

In figure 1 the arrows represent the directions of these transactions.

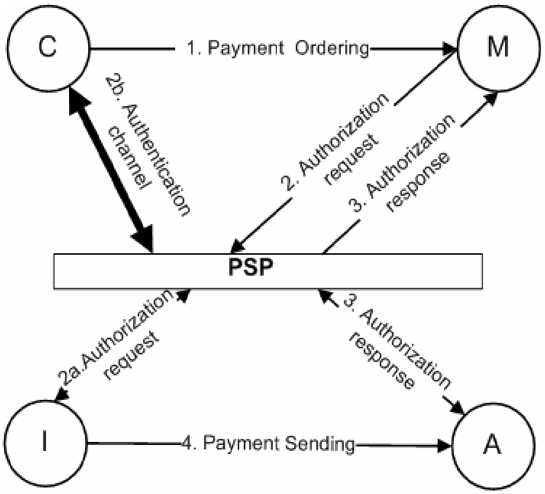

Fig. 1. Flow of messages in the traditional e-payment system

3 Extending Electronic Payment Model

3.1 New Technological Aspects Involved in Electronic Payment

Although, many scenarios have been described taking the traditional model as reference, we consider that it presents some limitations when describing actual electronic payment systems in which appear new technological aspects, such as: smart cards with network capabilities, handheld devices with reduced connectivity, business mediators with advantage services, multiplicity of involved entities.

Payment Network Smart Card (NSC)

Recently, many efforts have been made to transform the smart card into a device open to network interconnectivity. In order to do this, one must consider it as a fully functional Internet node in accordance, whenever possible, with established standards. Several works have been done to this field, such as that collected in [8], which has been oriented towards establishing a simplified TCP/IP protocol stack. Moreover, in [9] the authors aimed to provide a TCP-type protocol.

Although the resulting protocol did not fulfill all of the requirements established in the standard [10], it included the concept of agent-based Internet card. In [11], a review of the characteristics, steps and planning of what could be a new generation of smart cards with or without contacts is addressed. A clear evolution towards a networked smart card was quite evident. In [12] and [13], the card was already thought of as an Internet node which implemented standardized security and communication protocols, to be connected to a network via the host. The card was able to provide services or access Internet resources making use of protocol stacks in the same way as any other node on the network. Its use in security solutions was soon proposed. In this way, the network smart card was able to establish secure direct communication with remote Internet servers, as shown in [14][15]. This capacity allows the cards to guarantee online transactions.

A new remote authentication protocol architecture for network smart cards is described in [16] aiming to cover the authentication process globally with the maximum assurance of security. Her main characteristics are: 1) Stand-alone supplicant: The smart card adopts the functionality of standalone supplicant vs. split supplicant [17], 2) Remote authentication protocol architecture: Atomic smart card authentication protocol design and end-to-end mutual authentication schema on layer 2 of the OSI model.

These NSCs are powerful devices for being used as payment cards in electronic commerce. It could be used to establish a secure mechanism to authenticate the client.

Business mediator

Although, in electronic commerce seemed to suggest that e-commerce transactions would result in decreased costs for buyers and sellers alike, and would therefore ultimately lead to the elimination of mediator reducing this term to a digital shop (e-shop) like a mediator between virtual and real worlds [18]. A careful analysis of the structure and functions of electronic marketplaces reveals a different picture. The electronic business mediator have appeared [19][20][21][22] providing many value-adding functions that cannot be easily substituted or ‘internalized’ through direct supplier-buyer dealings, and hence mediating parties may continue to play a significant role even in the e-commerce world.

In the payment process, the business mediator is usually considered as entity which secure the payment transaction, this means; it is associated with the PSP. However, in others works it is represented, as entity capable of, among other functionalities, decrease the customer operations [23], simplifying the amount of transactions [24], provide a centralized the connection with the *PSP* [25], and else. In all the case, it is represented an entity with advantage services to client and to merchants, this means; in the *business process*, and out of the secure financial process such as: the PSP.

Consequently, the business mediator inside the payment process needs to be considered of as a new entity different to the PSP. His integration could modify the transaction between the involved entities and could generate some different scenarios.

Connectivity

Protocols designed in recent years for mobile payment systems are based on a scenario where all entities are directly interconnected to one another. This scenario (formally called "Full connectivity scenario") offers advantages to protocol designers because it allows them to simplify the design and development of payment protocols without losing security guarantees. Nevertheless, this scenario does not consider situations in which one of the engaging entities can not directly communicate with the other due to the impossibility of one of them to connect to Internet, maybe for restrictions of handheld device, geographic situation, etc. Considering previous works, these new scenarios of connectivity can be classified [26] as:

- *Disconnected*: *C* and *M* are disconnected from the *PSP* and directly communicate with each other using a local link.
- *Server-Centric:* The *PSP* is connected to both *C* and *M* but they are not directly connected with each other.
- *Client-Centric* [27]: *C* is connected to both *M* and the *PSP* but they are not directly connected with each other.
- *Kiosk-Centric* [28]: *M* is connected to both *C* and the *PSP* but they are not directly connected with each other.
- *Full-Connectivity:* All the entities are directly connected to one another.

Connectivity is one of the more important aspects which will determine the design of further security solutions for electronic payment, especially in mobile contexts. This concept implies in many cases new messages flow and new secure mechanisms to protect the traditional payment transactions.

Multiplicity of involved entities

Multiparty scenarios in electronic commerce [29] [30] are already well-know. Applications such as *virtual mall* or *market place, commercial search agent* describe a commerce scenario of multi-purchase, where one customer could interact with many merchants simultaneously; this means that it could obtain products from many merchants. In other business models, such as *demand aggregation*, appear scenarios where many customers need to form a partnership in order to increase their bargaining power and obtain discounts; in that way, finally this multiple customers could interact with one merchant of with many merchants, simultaneously.

Consequently, traditional topologies such as (one-to-many, ring, mesh, many-to-many) need to be considered in the payment model, and also, need to be integrated with the others previous aspects in order to represent real applications.

In that way, we propose to extend the electronic payment model to include these new aspects.

3.2 Extended E-Payment Model

Here, we will extend the electronic payment definition as the interactions between seven engaging parties (figure 2), three of which (I, A, PSP) remain unchanged from the classical model. Appear two new optional entities: (the dotted line around them represents that they may or may not be present) the business mediator (*Md*) and an enhanced payment card (NSC) with networking capabilities. The single merchant (M) is extended to one or more merchants (M+), and the client (C) is extended to one or more customers (C+).

The variety of connectivity conditions between the entities, are represented by arrows. It can be always direct connection, always indirect connection or one of them depending on the scenario.

The new entity Network smart card (*NSC*) needs a direct connection with the client (this means that the cardholder needs a mechanism to read the NSC). But although, the NSC could establish a direct authentication channel with his issuer bank, this connection could be by indirect communication channel.

And on the other hand, the mediator is located between *M+* and *C+*, since he could offer advantageous services, in the payment process, to both of them. Note that it is a different entity from *PSP*. In that way, his connection with all close entities (C+, M+, PSP) could by direct or indirect.

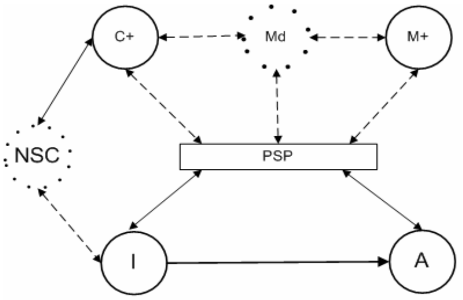

Fig. 2. Graphic representation of the extended e-payment model

In this case, inside the definition it is not possible to describe the flow of message because this one will depend on the involved entities and the type of connectivity (direct or indirect) between them. Due to that, in the next section, we describe two payment scenarios and the appropriate flow of messages. These scenarios could be derivated from the extended e-payment model, and could integrate all the new features.

4 New E-Payment Scenarios

Based on the new definition of the e-payment model we can generate a wide range of scenarios. We are interested in describing two novel scenarios where these new features are involved.

4.1 Client-Centric Payment with Multiple Merchants, Business Mediator, and Offline NSC (CC-M+ Payment)

This scenario (Figure 3.) could be described by the flow of messages and the participating entities as: one client (*C*), one business mediator (*Md*), multiple merchants

($M_i \in M$) and the *PSP* who provide the connection with the financial institutions (issuer and acquirer). The mediator plays the role of a virtual mall where the client can purchase products/services from different merchants. But especially, he acts as mediator between client and merchants, facilitating multi-purchases and multi-payment. In that way, *C* will delegate the multiple transactions with the merchants to *Md*.

However, the principal characteristic of this scenario is that the merchants and the *Md* are disconnected from the *PSP*, and only the *C* establishes a connection with this one. In that way, all the payment process, and the payment authorization process (requests and responses) need to flow through *C*. Due to that, the mediator could provide a single message as an appropriate combination of request/response messages. Finally, the client establishes a direct connection with the PSP, and he could directly send his private payment info to the PSP. The online authentication process could be completed with the authorization request process. In this scenario the payment process occurs in the following way:

1. The client sends the **payment order** *(PO)* to *Md*. In this case, this payment order could be composed by multiple payment orders PO_i to each merchant $Mi \in M+$, where *M+* are the merchants selected by the client.

2. Once this payment order *PO* is received, the mediator split it in a number of PO_i and **distributes** it to each involved merchant $Mi \in M'$.

3. Afterwards, when merchants receive the payment order *POi,* they start with the **authorization request** *ARi* to the *PSP*. Since they have not connectivity with the *PSP*, they need to do the process through *Md.*

4. In this moment, the *Md* waits for all the authorization request *ARi* which is send by the involved merchants $Mi \in M'$. Once *Md* receives AR_i , it creates a single a single **authorization request** message and **forwards** it to *C***.**

5. *C* has the responsibility to connect to the *PSP* and to send all the **authorization requests** received from merchants through *Md.*

6. Upon reception of the message from *C*, the *PSP* could receive in this scenario the **authentication** information of C. And for that, he continues with the traditional responsibility of checking the authenticity of *C* by means of the issuer bank. After which, PSP sends the **authorization response** *ARs*. This will be composed by the responses *ARsi* to each involved merchants $Mi \in M+$. This *ARs* need to be sent through *C*.

7. The client receives the products/services when all involved merchants receive the **authorization response** *ARsi*. Due to that, *C* **forward** the *ARs* received from *PSP* to *Md.*

8. Finally, *Md* divides the message *ARs* and **distributes** the appropriate **authorization responses** *ARsi* to each involved merchants $Mi \in M+$.

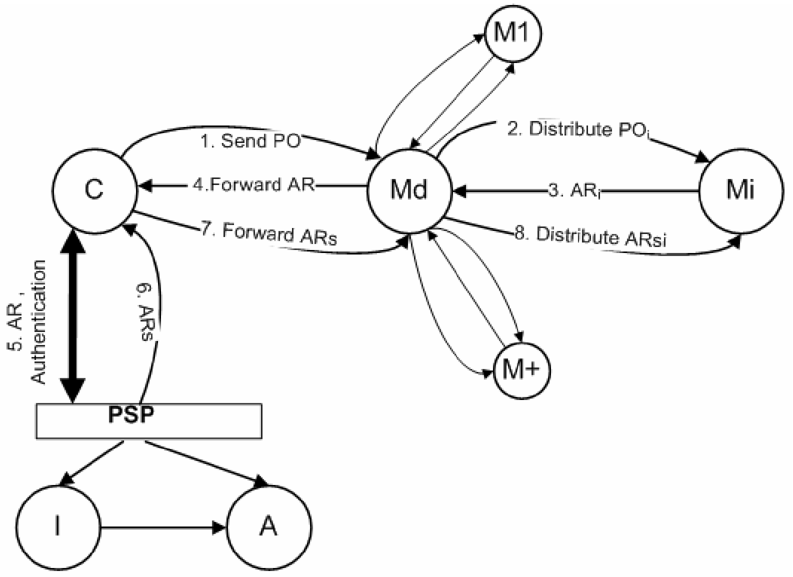

Fig. 3. Flow of messages in CC-M+ scenario

4.2 Client-Centric Payment with Multiple Merchants, Business Mediated, and Online NSC (CC-M+-NSC)

This new scenario (Figure 4.) could be described, as in the previous case as: a client (*C*), a business mediator (*Md*) and multiple merchants ($M_i \in M$) and the *PSP,* who provides the connection with the financial institutions (issuer and acquirer). The mediator plays the same role. And in the same way that in the previous one, the merchants and the *Md* are disconnected from the *PSP*. Only the *C* can communicate with the *PSP*. However in this scenario a new entity appears: an online NSC which has the possibility of directly authenticating the client with the issuer bank. In that way, the flow of payment process is transformed in the following way:

- The steps, from 1 to 4, are repeated in this scenario. Nevertheless, the step 5 introduce new variant.

5. *C* has the responsibility of connecting with the *PSP* to send all the **authorization requests** received from merchants through *Md*. The authentication channel is now provided by the NSC

6. Upon reception of a message from *C*, the *PSP* translate the authentication mechanism to the issuer bank...

7. Now the authentication process is handle by the NSC established an **authentication channel,** between NSC and I.

8. When all this process concludes (and the PSP receive the issuer response), the PSP sends the **authorization response** *ARs* (composed by the responses *ARsi*) to each involved merchants *Mi*∈*M'* through *C*.

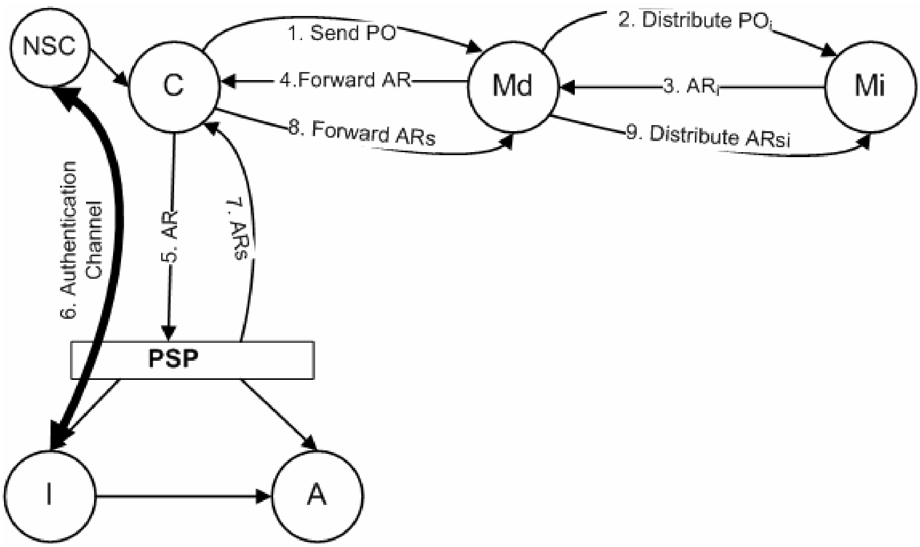

Fig. 4. Flow of message in the CC-M+-NSC payment scenario

9. *C* **forward** the *ARs* received from *PSP* to *Md.*

10. And Finally, *Md* split the message *ARs* and **distributes** the appropriate **authorization responses** *ARsi* to each involved merchants *Mi∈M'*.

5 New Security Requirements for the Extended Version of the Payment Model

Payment requires the greatest level of security in electronic commerce transactions [31][32]. For this reason, a solution is needed that guarantees confidentiality, authenticity, integrity and non-repudiation of the transactions. However, many new requirements need to be considered in our models. Now we enumerate those security requirements according to the new features.

Payment Network Smart Card

- A protected channel (confidential, authenticated and keeping integrity) should be built by own network smart card and the remote server (Access Control server controlled by the issuer bank).
- Standardized communication and transport protocols between the smart card and the issuer bank with security purpose.

Business mediator

- A secure architecture to create a trust relationship with the un-trusted *Md.*
- A secure mechanism to assign authorization to *Md*, for distributing the payment order, for joining the authorization request and, next for distributing the authorization responses for each involved merchant.

- A mechanism to create a non repudiation evidence of *Md's* participation in each step of the protocol.
- A mechanism to establish mutual authentication schemes between customer and merchants across untrustworthy mediator.

Connectivity

- A mechanism to guarantee the security of the message when going through one or many entities. For example all the authorization process messages through *Md*, and *C* to *PSP*.
- A secure mechanism to exchange cryptographic information, such as, a public key or a symmetric key, without online connectivity.

Multiplicity of involved merchants

- A mechanism to protect the confidentiality of the purchases and payment information between all involved merchants, in order to avoid that some malicious involved merchant could eavesdrop the information sent to other legitimate merchant.
- A mechanism to protect the integrity of the purchases and payment information, which is sent to the merchants. With the goal to of avoiding that some malicious merchant could modify the information sent to other merchants.
- A mechanism to avoid mutual coordination, between the involved entities, to carry malicious behaviors.

6 Conclusion

Security in traditional e-payment model is based on protecting the transaction flow between business entities (client and merchant) and their transactions with the financial institutions. However, the security architectures based on this model are not sufficiently robust when new participants with their respective functionalities and particularities engage the e-payment system.

In this paper we summarize four new aspects (payment network smart card, connectivity, business mediator, multiplicity of involved entities) to consider an extended version of traditional payment model.

Also, we describe two new payment scenarios (*Client-Centric payment with multiple merchants, business mediator, and offline NSC*, and, *Client-Centric payment with multiple merchants, business mediator, and online NSC*) in order to demonstrate how these new aspects could define new payment interactions and consequently requires new security solutions. A brief discussion of the security requirements of these scenarios allow us to how that it is not trivial to adapt the current payment solution to these new approach. In the future we are interested in developing a realistic secure payment solution for the proposed scenarios based on an extended version of the traditinal payment solutions.

References

1. Kungpisdan, S.: Modelling, design, and analysis of Secure Mobile Payment Systems., Thesis for Doctor of Philosophy, Faculty of Information Technology, Monash University (2005), http://beast.csse.monash.edu.au/~srini/theses/keng.pdf
2. 3-D Secure. System Overview. 70015-01 External Version Copyright © 2002-2003. Visa International Version 1.0.2 (May 01, 2003), http://partnernetwork.visa.com/pf/3dsec/download/trk_3dsec_system_overview_v102.pdf
3. Kou, W.: Payment technologies for e-commerce. Springer, Heidelberg (2003)
4. O'Mahony, D.: Electronic payment systems for e-commerce. Artech House (2001)
5. Secure system to pay with mobile phone charging the amount directly to a payment card, http://www.mobipay.com
6. Secure online payment gateway: PayPal, http://www.paypal.com
7. Payment gateway: Authorize.Net, http://www.authorizenet.com/
8. Rees, J., Honeyman, P.: Webcard: a Java Card web server. In: Proc. of 4th IFIP Smart Card Research and Advanced Application Conference, CARDIS 2000, Bristol, U.K (2000)
9. Urien, P.: Internet card, a smart card as a true Internet node. Computer Communications 23(17), 1655–1666 (2000)
10. Postel, J.: Transmission Control Protocol. IETF RFC 079 (September 1981)
11. IST Project RESET, Roadmap for European Research on Smartcard related Technologies, IST-2001-39046: Final Roadmap, v.5 (May 2003)
12. Montgomery, M., Ali, A., 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 2004, Toulouse, France, August 23-26, 2004. Kluwer Academic Publishers, Dordrecht (2004)
13. Lu, H.K.: New Advances in Smart Card Communications, International Conference on Computing. In: Communications and Control technologies (CCCT), Austin, TX, USA, August 14-17 (2004)
14. Lu, H.K., Ali, A.: Prevent On-line Identity Theft - Using Network Smart Cards for Secure On-line Transactions. In: Zhang, K., Zheng, Y. (eds.) ISC 2004. LNCS, vol. 3225. Springer, Heidelberg (2004)
15. Ali, A., Lu, K., Montgomery, M.: Network Smart Card: A New Paradigm of Secure Online Transactions. In: Proc. of Security and Privacy in the Age of Ubiquitous Computing, IFIP TC11 20th International Conference on Information Security (SEC 2005), Chiba, Japan, May 30 - June 1 (2005)
16. Torres, J., Izquierdo, A., Sierra, J.M.: Advances in network smart cards authentication. Computer Networks 51(9), 2249–2261 (2007)
17. Torres, J., Izquierdo, A., Sierra, J.M., Ribagorda, A.: Towards selfauthenticable smart cards. Computer Communications 29(15), 2781–2787 (2006)
18. Porter, M.: Strategy and the Internet. Harvard Business Review, 63–78 (March 2001)
19. Giaglis, G., Klein, S., O'Keefe, R.: The role of intermediaries in electronic marketplaces: developing a contingency model. Information Systems Journal 12(3), 231 (2002)
20. Dikaiakos, M.: Intermediary infrastructures for the World Wide Web. Computer Networks 45(4), 421–447 (2004)
21. Esparza, O., Muñoz, J., Soriano, M., Forné, J.: Secure brokerage mechanisms for mobile electronic commerce. Computer Communications 29(12), 2308–2321 (2006)
22. Bhargava, H., Choudhary, V.: Economics of an Information Intermediary with Aggregation Benefits. Information Systems Research 15(1), 22–36 (2004)

23. Bhargava, H., Choudhary, V.: Economics of an Information Intermediary with Aggregation Benefits. Information Systems Research 15(1), 22–36 (2004)
24. Wang, Y., Varadharajan, V.: A mobile autonomous agent-based secure payment protocol supporting multiple payments. In: IAT 2005, pp. 88–94 (2005)
25. Carbonell, M., Sierra, J., Torres, J., Izquierdo, A.: Security analysis of a new multi-party payment protocol with intermediary service. In: DEXA Workshops 2007, pp. 698–702 (2007)
26. Chari, S., Kermani, P., Smith, S., Tassiulas, L.: Security Issues in MCommerce: An Usage-Based Taxonomy. In: Proceedings of E-Commerce Agents, pp. 264–282 (2001)
27. Tellez Isaac, J., Sierra Cámara, J.M.: Anonymous Payment in a Client Centric Model for Digital Ecosystems. In: Proceedings of IEEE International Digital Ecosystems and Technologies (DEST), Australia (2007)
28. Tellez, J., Sierra, J.M., Izquierdo, A., Torres, J.: Anonymous Payment in a Kiosk Centric Model using Digital signature scheme with message recovery and Low Computional Power Devices. Journal of Theorical and Applied Electronic Commerce Research 1(2), 1–11 (2006)
29. Bartelt, A., Lamersdorf, W.: A multi-criteria taxonomy of business models in electronic commerce. In: Fiege, L., Mühl, G., Wilhelm, U.G. (eds.) WELCOM 2001. LNCS, vol. 2232, pp. 193–205. Springer, Heidelberg (2001)
30. Rappa, M.: Business models on the web. Managing the digital enterprise(October 2006), http://digitalenterprise.org/models/models.html
31. Stallings, W.: Cryptography and network security: principles and practices, ch. 16-20. Prentice Hall, Englewood Cliffs (2006)
32. Tsiakis, T., Stheohanidews, G.: The concept f security and trust in electronic payments. Computer & Security 24(1), 10–15 (2005)