Giuseppe Psaila
Roland Wagner (Eds.)

LNCS 4655

E-Commerce and Web Technologies

8th International Conference, EC-Web 2007
Regensburg, Germany, September 2007
Proceedings

Springer

Giuseppe Psaila Roland Wagner (Eds.)

E-Commerce and Web Technologies

8th International Conference, EC-Web 2007
Regensburg, Germany, September 3-7, 2007
Proceedings

Springer

Volume Editors

Giuseppe Psaila
Università degli studi di Bergamo
Facoltà di Ingegneria, Viale Marconi 5, 24044 Sede di Dalmine (BG), Italy
E-mail: psaila@unibg.it

Roland Wagner
University of Linz
Institute of FAW
Altenbergerstrasse 69, 4040 Linz, Austria
E-mail: rrwagner@faw.uni-linz.ac.at

Library of Congress Control Number: 2007933402

CR Subject Classification (1998): H.4, K.4.4, J.1, K.5, H.3, H.2, H.2.5, K.6.5

LNCS Sublibrary: SL 3 – Information Systems and Application, incl. Internet/Web and HCI

ISSN 0302-9743
ISBN-10 3-540-74562-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74562-4 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12115075 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4655

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Preface

Welcome to EC-Web 2007, the International Conference on E-commerce and Web Technologies. As in the past 7 years, EC-Web was co-located with DEXA, the International Conference on Database and Expert Systems Applications, and took place in Regensburg, a very beautiful city in the heart of Europe.

This was the eighth edition of EC-Web, and we think that it is now a mature conference. It gained a stable audience and it is considered by several authors as a key conference for publishing their ideas and their work.

The new Chairs, Roland Wagner and Giuseppe Psaila, followed the line of evolution to make the conference even more attractive. In fact, one key feature of EC-Web is the two-fold nature of the conference: it brings together both papers proposing technological solutions for E-commerce and the World Wide Web, and papers concerning management of E-commerce, such as Web marketing, impact of E-commerce on business processes and organizations, analysis of case studies. This year, the new topic of "social aspects" was introduced: in fact, the every-day increasing availability of E-commerce solutions for consumers is causing the rise of new behaviors that must be studied, in order to understand the impact of E-commerce solutions on every-day life and the new opportunities that these new behaviors open.

The second significant change introduced this year was the number of reviewers: the Program Committee was composed of more than 120 reviewers (instead of 60 reviewers in the last edition). This choice was motivated by the wish to provide a better service to authors and improve the quality of the selection process.

The technical program, comprised 22 papers selected among 67 submitted papers, with a selection rate of 32%. The contributions covered several interesting areas, such as security and privacy, Web services, recommender systems, Web marketing, profiling and customer behavior, electronic commerce technology, impact of E-commerce on organizations.

We think the program is interesting and we hope the readers think the same.

June 2007

Giuseppe Psaila
Roland R. Wagner

Organization

Program Committee Chairpersons

Giuseppe Psaila, University of Bergamo, Italy
Roland Wagner, FAW, University of Linz, Austria

Program Committee

Marco Aiello, Rijksuniversiteit Groningen, The Netherlands
Esma Aïmeur, University of Montreal, Canada
Damminda Alahakoon, Monash University, Australia
Sergio Alonso, University of Granada, Spain
Jörn Altmann, Seoul National University, South-Korea and Intl. University of Bruchsal, Germany
Sami Bhiri, DERI, Ireland
Sourav S. Bhowmick, Nanyang Technological University, Singapore
Enrique Bigné, University of Valencia, Spain
Susanne Boll, University of Oldenburg, Germany
Michelangelo Ceci, University of Basi, Italy
Wojciech Cellary, Poznan University of Economics, Poland
Francisco Chiclana, De Montfort University, UK
Jen-Yao Chung, IBM T.J. Watson Research Center, USA
Andrzej Cichocki, Telcordia Technologies, USA
Kajal Claypool, Oracle, USA
Emmanuel Coquery, University Lyon 1, France
Arthur I. Csetenyi, Budapest Corvinus University, Hungary
Alfredo Cuzzocrea, University of Calabria, Italy
Simão Melo de Sousa, University of Beira Interior, Portugal
Radoslav Delina, Technical University of Kosice, Slovakia
Tommaso Di Noia, Politecnico di Bari, Italy
Schahram Dustdar, Vienna University of Technology, Austria
Johann Eder, University of Vienna, Austria
Maria Jose Escalona, Universidad de Sevilla, Spain
Torsten Eymann, University of Bayreuth, Germany
Eduardo Fernandez, Florida Atlantic University, USA
Gianluigi Ferrari, University of Pisa, Italy
Elena Ferrari, University of Insubria at Como, Italy
Ludger Fiege, Siemens, Germany
Carlos Flavian, University of Zaragoza, Spain
Farshad Fotouhi, Wayne State University, USA
Eduard Cristóbal Fransi, University of Lleida, Spain
Yongjian Fu, Cleveland State University, USA

Walid Gaaloul, DERI, Ireland
Stephane Gagnon, Université du Québec en Outaouais (UQO), Canada
Jing Gao, University of South Australia, Australia
Peter Geczy, AIST, Japan
Chanan Glezer, Ben Gurion University, Israel
Claude Godart, University of Nancy and INRIA, France
Mohand-Said Hacid, University Lyon 1, France
G. Harindranath, University of London, UK
Aboul Ella Hassanien, Kuwait University, Kuwait
Josef Herget, University of Chur, Switzerland
Enrique Herrera-Viedma, University of Granada, Spain
Klaus Herrmann, University of Stuttgart, Germany
Charles Hofacker, Florida State University, USA
Yigal Hoffner, IBM Zurich Research Lab., Switzerland
Birgit Hofreiter, University of Vienna, Austria
Christian Huemer, Vienna University of Technology, Austria
Michael C. Jaeger, Berlin University of Technology, Germany
Dimka Karastoyanova, University of Stuttgart, Germany
Gregory E. Kersten, Concordia University Montreal, Canada
Hiroyuki Kitagawa, University of Tsukuba, Japan
Jan Klas, University of Economics, Prague, Czech Republic
Gabriele Kotsis, Johannes Kepler University Linz, Austria
Sandeep Krishnamurthy, University of Washington, USA
Alberto Laender, Federal University of Minas Gerais, Brazil
Deok Gyu Lee, Electronics and Telecommunications Research Institute(ETRI), Korea
Juhnyoung Lee, IBM T.J. Watson Research Center, USA
Joerg Leukel, University of Hohenheim, Germany
Leszek T. Lilien, Western Michigan University, USA
Ee-Peng Lim, Nanyang Technological University, Singapore
Huan Liu, Arizona State University, USA
Antonio Gabriel Lopez, University of Granada, Spain
Heiko Ludwig, IBM T.J. Watson Research Center, USA
Sanjay Kumar Madria, University of Missouri-Rolla, USA
Koné Mamadou Tadiou, Université Laval, Canada
Mário Marques Freire, University of Beira Interior, Portugal
Luis Martínez Lopez, University of Jaen, Spain
Francisco Mata Mata, University of Jaen, Spain
Massimo Mecella, University of Rome La Sapienza, Italy
Bamshad Mobasher, DePaul University, USA
Mukesh Mohania, IBM India Research Lab, India
Gero Muehl, TU Berlin, Germany
Guenter Mueller, University of Freiburg, Germany
Dirk Neumann, University of Karlsruhe, Germany
Wee-Keong Ng, Nanyang Tech. University, Singapore
Anne-Marie Oostveen, Oxford Internet Institute, UK
Rolf Oppliger, eSECURITY Technologies, Switzerland
Stefano Paraboschi, University of Bergamo, Italy

Jong Hyuk Park, Hanwha S&C Co., Ltd., Korea
Oscar Pastor, Valencia University of Technology, Spain
Vicente Pelechano, Techical University of Valencia, Spain
Günther Pernul, University of Regensburg, Germany
Ilia Petrov, SAP, Germany
Dimitris Plexousakis, University of Crete, Greece
Ivana Podnar Zarko, FER, University of Zagreb, Croatia
Birgit Proell, Johannes Kepler University Linz, Austria
Gerald Quirchmayr, University of Vienna, Austria
Indrakshi Ray, Colorado State University, USA
Werner Retschitzegger, Johannes Kepler University Linz, Austria
Inmaculada Rodríguez-Ardura, Universitat Oberta de Catalunya, Spain
Jarogniew Rykowski, Poznan University of Economics, Poland
Tomas Sabol, Technical University of Kosice, Slovakia
Paolo Salvaneschi, University of Bergamo, Italy
Nandlal L. Sarda, Indian Institute of Tech. Bombay, India
Thorsten Scheibler, University of Stuttgart, Germany
Eusebio Scornavacca, Victoria University of Wellington, New Zealand
Huseyin Seker, De Montfort University, UK
Martin Smits, Tilburg University, The Netherlands
Steffen Staab, University of Koblenz, Germany
Michael Stroebel, BMW Group, Germany
Junichi Suzuki, University of Massachusetts, Boston, USA
Roger M. Tagg, University of South Australia, Australia
Kian-Lee Tan, National University of Singapore, Singapore
Samir Tata, Institut National des télécommunications, France
Stephanie Teufel, University of Fribourg, Switzerland
Bartel Van de Walle, Tilburg University, The Netherlands
Willem Jan van den Heuvel, Tilburg University, The Netherlands
Aad van Moorsel, Newcastle University, UK
Krishnamurthy Vidyasankar, Memorial University of Newfoundland, Canada
Emilija Vuksanovic, University of Kragujevac, Serbia
Hans Weigand, Tilburg University, The Netherlands
Matthias Werner, TU Berlin, Germany
Hannes Werthner, Technical University of Vienna, Austria
Janusz Wielki, Opole University of Technology, Poland
Hongji Yang, De Montfort University, UK
Ilya Zaihrayeu, University of Trento, Italy
Olaf Zimmerman, IBM Zurich, Switzerland

Acknowledgement

The work was supported by the PRIN 2006 program of the Italian Ministry of Research, within project "Basi di dati crittografate" (2006099978).

Lecture Notes in Computer Science

For information about Vols. 1–4575

please contact your bookseller or Springer

Vol. 4720: B. Konev, F. Wolter (Eds.), Frontiers of Combining Systems. X, 2283 pages. 2007. (Sublibrary LNAI).

Vol. 4708: L. Kučera, A. Kučera (Eds.), Mathematical Foundations of Computer Science 2007. XVIII, 764 pages. 2007.

Vol. 4707: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part III. XXIV, 1205 pages. 2007.

Vol. 4706: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part II. XXIII, 1129 pages. 2007.

Vol. 4705: O. Gervasi, M.L. Gavrilova (Eds.), Computational Science and Its Applications – ICCSA 2007, Part I. XLIV, 1169 pages. 2007.

Vol. 4703: L. Caires, V.T. Vasconcelos (Eds.), CONCUR 2007 – Concurrency Theory. XIII, 507 pages. 2007.

Vol. 4697: L. Choi, Y. Paek, S. Cho (Eds.), Advances in Computer Systems Architecture. XIII, 400 pages. 2007.

Vol. 4685: D.J. Veit, J. Altmann (Eds.), Grid Economics and Business Models. XII, 201 pages. 2007.

Vol. 4683: L. Kang, Y. Liu, S. Zeng (Eds.), Intelligence Computation and Applications. XVII, 663 pages. 2007.

Vol. 4682: D.-S. Huang, L. Heutte, M. Loog (Eds.), Advanced Intelligent Computing Theories and Applications. XXVII, 1373 pages. 2007. (Sublibrary LNAI).

Vol. 4681: D.-S. Huang, L. Heutte, M. Loog (Eds.), Advanced Intelligent Computing Theories and Applications. XXVI, 1379 pages. 2007.

Vol. 4679: A.L. Yuille, S.-C. Zhu, D. Cremers, Y. Wang (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 494 pages. 2007.

Vol. 4678: J. Blanc-Talon, W. Philips, D. Popescu, P. Scheunders (Eds.), Advanced Concepts for Intelligent Vision Systems. XXIII, 1100 pages. 2007.

Vol. 4673: W.G. Kropatsch, M. Kampel, A. Hanbury (Eds.), Computer Analysis of Images and Patterns. XX, 1006 pages. 2007.

Vol. 4671: V. Malyshkin (Ed.), Parallel Computing Technologies. XIV, 635 pages. 2007.

Vol. 4660: S. Džeroski, J. Todorovski (Eds.), Computational Discovery of Scientific Knowledge. X, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4656: M.A. Wimmer, J. Scholl, Å. Grönlund (Eds.), Electronic Government. XIV, 450 pages. 2007.

Vol. 4655: G. Psaila, R. Wagner (Eds.), E-Commerce and Web Technologies. XIII, 229 pages. 2007.

Vol. 4654: I.Y. Song, J. Eder, T.M. Nguyen (Eds.), Data Warehousing and Knowledge Discovery. XVI, 482 pages. 2007.

Vol. 4651: F. Azevedo, P. Barahona, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 185 pages. 2007. (Sublibrary LNAI).

Vol. 4649: V. Diekert, M.V. Volkov, A. Voronkov (Eds.), Computer Science – Theory and Applications. XIII, 420 pages. 2007.

Vol. 4647: R. Martin, M. Sabin, J. Winkler (Eds.), Mathematics of Surfaces XII. IX, 509 pages. 2007.

Vol. 4645: R. Giancarlo, S. Hannenhalli (Eds.), Algorithms in Bioinformatics. XIII, 432 pages. 2007. (Sublibrary LNBI).

Vol. 4644: N. Azemard, L. Svensson (Eds.), Integrated Circuit and System Design. XIV, 583 pages. 2007.

Vol. 4643: M.-F. Sagot, M.E.M.T. Walter (Eds.), Advances in Bioinformatics and Computational Biology. XII, 177 pages. 2007. (Sublibrary LNBI).

Vol. 4642: S.-W. Lee, S.Z. Li (Eds.), Advances in Biometrics. XX, 1216 pages. 2007.

Vol. 4641: A.-M. Kermarrec, L. Bougé, T. Priol (Eds.), Euro-Par 2007 Parallel Processing. XXVII, 974 pages. 2007.

Vol. 4639: E. Csuhaj-Varjú, Z. Ésik (Eds.), Fundamentals of Computation Theory. XIV, 508 pages. 2007.

Vol. 4638: T. Stützle, M. Birattari, H.H. Hoos (Eds.), Engineering Stochastic Local Search Algorithms. X, 223 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4635: B. Kokinov, D.C. Richardson, T.R. Roth-Berghofer, L. Vieu (Eds.), Modeling and Using Context. XIV, 574 pages. 2007. (Sublibrary LNAI).

Vol. 4634: H.R. Nielson, G. Filé (Eds.), Static Analysis. XI, 469 pages. 2007.

Vol. 4633: M. Kamel, A. Campilho (Eds.), Image Analysis and Recognition. XII, 1312 pages. 2007.

Vol. 4632: R. Alhajj, H. Gao, X. Li, J. Li, O.R. Zaïane (Eds.), Advanced Data Mining and Applications. XV, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4628: L.N. de Castro, F.J. Von Zuben, H. Knidel (Eds.), Artificial Immune Systems. XII, 438 pages. 2007.

Vol. 4627: M. Charikar, K. Jansen, O. Reingold, J.D.P. Rolim (Eds.), Approximation, Randomization, and Combinatorial Optimization. XII, 626 pages. 2007.

Table of Contents

Security and Privacy

Profiling and Customer Behaviour

Evaluation of E-Commerce Impact

Recommender Systems and E-Negotiations

Web Services

E-Commerece and Organizations

Web Marketing

EC Technology

A Secure Payment Protocol for Restricted Connectivity Scenarios in M-Commerce

Jesús Téllez Isaac[1] and José Sierra Camara[2]

[1] Universidad de Carabobo, Computer Science Department (Facyt)
Av. Universidad, Sector Bárbula, Valencia, Venezuela
jtellez@uc.edu.ve
[2] Universidad Carlos III de Madrid, Computer Science Department,
Avda. de la Universidad, 30, 28911, Leganés (Madrid), Spain
sierra@inf.uc3m.es

Abstract. A significant number of mobile payment systems have been proposed in recent years, most of them based on a scenario where all the entities are directly connected one to another (formally called "Full connectivity scenario"). Despite of the advantages that the aforementioned scenario offers to protocol's designers, regarding design simplification and development of payment protocols without losing security capabilities, the full connectivity scenario does not consider those situations in which the client cannot directly communicate with the issuer (Kiosk Centric Model) or the merchant has no direct communication with the acquirer (Client Centric Model). In order to overcome this restriction and contribute to the progress of m-commerce, in this paper we propose an anonymous protocol that uses a digital signature scheme with message recovery using self-certified public keys that is suitable for both the Kiosk Centric Model and Client Centric Model. As a result, our proposal shows that m-commerce is possible in restrictive connectivity scenarios, achieving the same security capabilities than other protocols designed for mobile payment systems based on "Full connectivity scenario".

Keywords: Payment Protocol, Self-certified public keys, Digital Signature with message recovery, Mobile Payment System.

1 Introduction

Several mobile payment systems have emerged in the last years which allow payments for services and goods from mobile devices using different kinds of payments: credit-card payments, micropayments and digital coins. The relationship between payee and acquirer is quite strict in most of these mobile payment systems and does not allow the use of schemes in which the communication among these parties is not possible due to: 1) the impossibility of the merchant to connect to Internet and 2) the high costs and/or inconveniences of using the infrastructure necessary to implement other mechanisms of communication between the merchant and the acquirer (such SMS, phone call, etc.).

G. Psaila and R. Wagner (Eds.): EC-Web 2007, LNCS 4655, pp. 1–10, 2007.

The above restrictions do not represent an important issue for the majority of mobile payment systems proposed up until now because they assume that engaging parties are able to connect to Internet. Nevertheless, in the real world there are some situations that the merchant meets in which it is not possible to connect to the Internet, so it becomes necessary to develop mobile payment systems where the payee could sell goods/services even thought he/she may not have Internet access.

According to our operational models (where client cannot communicate directly with issuer, or merchant cannot communicate with the acquirer in a direct way, the traditional digital signature schemes based on asymmetric techniques are not suitable because one party (client or merchant, depending on the scenario) has connectivity restrictions and consequently, communication with others parties (as a CA, for verifying a certificate) is not possible during a purchase. Therefore, usage of a non-traditional digital signature scheme is required in order to satisfy our requirements.

In order to eliminate the restriction of those mobile payment systems based on the Full Connectivity Scenario regarding the direct communication between client and issuer, and among merchant and acquirer for authentication purposes, in section 3, we design a protocol that allows to a party (A) to send a message to another peer (B) through a third party (who will not be able to decrypt this message) in the those scenarios. The proposed protocol employs the authentication encryption scheme proposed by [13] that allows only specified receivers to verify and recover the message, so any other receiver will not be able to access the information. Moreover, it supports both credit-card and debit-card transactions and protects the real identity of the clients during the purchase. As a result, our proposal represents an alternative to other mobile payment systems with restrictions regarding a mandatory connection among two of its parties.

Outline of this paper: We begin by presenting the related work. Then, we present our approach which includes a complete list of notations, the operational model and the proposed protocol. In section 4, a security analysis of the proposed protocol is presented. We end this paper with the conclusions in section 5.

2 Related Work

Recently, [3] conducted a research that unifies many proposed m–commerce usages into a single framework. This research intended to revise the possible range of mobility scenarios, identifying the security issues for each connectivity scenario. As a result, five scenarios were identified and analyzed: Disconnected Interaction, Server Centric Case, Full Connectivity, Kiosk Centric Case and Client Centric Case. The last two have been considered as the starting point in the design of our proposal.

Most of the protocols proposed in recent years for the Full Connectivity scenario are based on public-key infrastructure (PKI) [1,4,8,12] whereas the remaining employ symmetric-key operations which is more suitable for wireless networks [7]. Unfortunately, usage of those protocols is not possible in scenarios

where direct interaction among two of its parties is not allowed due to the communication restriction imposed by the model (as happens in Kiosk Centric Model or Client Centric Model). However, some protocols could be reformulated to overcome this restriction (achieving the same security and performance levels, but in a different scenario), while being suitable for mobile payment systems with Restricted Connectivity. For example, Téllez *et al.* [9] reformulate the mobile payment protocol proposed by [7] to satisfy the requirements of their proposal.

A few number of signatures schemes with message recovery have been proposed in recent years which illustrate how a signer's public key can be simultaneously securely authenticated during the signature verification, avoiding communication with a Certificate Authority during a transaction in order to verify the validity of a certificate since the certificate is embedded in public key itself. Therefore, and as shown in [10], digital scheme signature schemes with message recovery are suitable for mobile payment protocols based on a restrictive connectivity scenarios like the one being suggested in this work.

3 Our Approach

3.1 Parties and Notations

All the entities involved in our protocol are called parties and communicate through wireless and wired network. The symbols C, M, PG, I, A are used to denote the names of the parties Client, Merchant, Payment Gateway, Issuer and Acquirer respectively. The following symbols are used to represent other messages and protocols:

- ID_P : the identity of party P that contains the contact information of P.
- NID_C : Client's nickname, temporary identity.
- K_P : party's K public key.
- K_S : party's K private key.
- $\mathrm{E}_{P-P'}(\mathrm{X})$: message X signed and encrypted by ID_P to a specified receiver $ID_{P'}$, following the generation procedure of signature proposed by [13].
- TID: Identity of transaction that includes time and date of the transaction.
- OI: Order information (OI = {TID, OD, h(OD, Price)}) where OD and Price are order descriptions and its amount.
- TC: The type of card used in the purchase process (TC={Credit, Debit}).
- TS: The type of scenario used during a payment (TC={Kiosk, Client})
- DCMA : The status of the direct connection between the merchant and the acquirer (DCMA = {Connected, NO-Connected}). The default value is *NO-Connected.*
- DCCI : The status of the direct connection between the client and the issuer (DCCI = {Connected, NO-Connected}). The default value is *NO-Connected.*
- Stt: The status of transaction (Stt = {Accepted, Rejected}).
- TIDReq : The request for TID.
- MIDReq : The request for ID_M.
- MPReq : The request for M_P.
- DCMAReq : The request for DCMA.
- $h(M)$: the one-way hash function of the message M.

3.2 Operational Model

Our operational models, Kiosk Centric Model and Client Centric Model (figure 1 and figure 2, respectively), are composed of five entities:

1. *Client*: a user who wants to buy goods or services from the merchant, equipped with a short range link (such Infrared, Wi-Fi or Bluetooth). Only in the Client Centric Model, the client is able to access Internet.
2. *Merchant*: a computational entity (such an intelligent vending machine) that offers or sells products or services to the client, and with which the user participates in a transaction using a short range link. In Kiosk Centric Model, this entity connects with the Payment Gateway through a secure channel allowing the merchant to communicate with the acquirer using this connection whereas in Client Centric Model, direct communication with the Issuer is not possible so it must take place through the client.
3. *Acquirer*: is the merchant's financial institution.
4. *Issuer*: is the customer's financial institution.
5. *Payment Gateway*: an additional entity that acts as a medium between acquirer/issuer at banking private network side and client/vendor at the Internet side for clearing purpose [7].

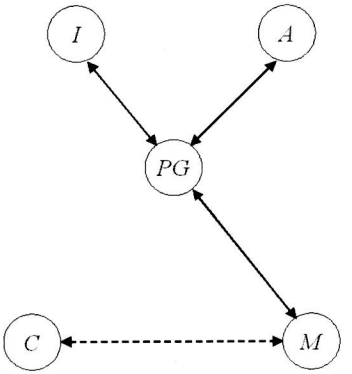

Fig. 1. Kiosk Centric Model

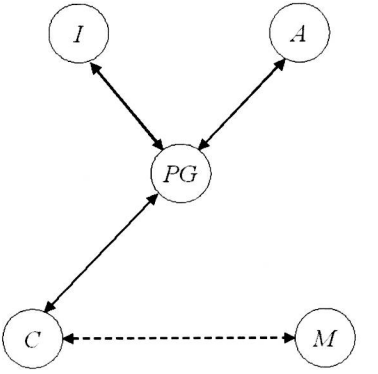

Fig. 2. Client Centric Model

The links among the five entities of our operational models are specified in figure 1 and 2. Note that, in both operational models, the connection between the client and the merchant (denoted as the dotted arrow) is setup up through a wireless channel.

On the other hand, interaction among client and payment gateway or between merchant and payment gateway (depicted as the solid arrow in any of the operational models) should be reliable and secure against passive and active attacks. Note that the issuer, acquirer and payment gateway operates under the banking private network, so the security of the messages exchanged among them is out of the scope of this paper.

3.3 Initial Assumptions

The initial assumptions for our proposed protocol can be stated as follows:

1. Client registers herself to an issuer before making payments. The registration can be done either personally at the issuer's premises or via the issuer's website. During the above process, the client shares her credit- and/or debit-card information (CDCI) with her issuer (who will not reveal it to any merchant). On the other hand, the issuer assigns several nicknames to the client and those nicknames are know only by the client and the issuer [6]. In the Kiosk Centric Model, the client sends (with the assistance of the issuer) her nicknames and x_C to SA and receives all system parameters from the SA.
2. The system authority (SA) is responsible for generation of the system parameters in the system initialization phase (as described in [13][11]).
3. Every party of the system P_i (whose identity is ID_{P_i}) choose a number K_{S_i} as her secret key and computes $x_i = g^{K_{S_i}} \bmod N$. Then, P_i sends (x_i, ID_{P_i}) to SA. After receiving (x_i, ID_{P_i}), the SA computes and publishes the public key of P_i as $K_{P_i}=(x_i - ID_{P_i})^{h^{-1}(ID_{P_i})} \bmod N$ [13]. As the client uses a nickname instead the real identity to protect her privacy, one K_{P_i} must be generated and published for every nickname assigned to the client.
4. The client holds C_S, ID_I, and system parameters in her mobile device. Also, in Kiosk Centric Model, client holds I_P.

3.4 Detailed Protocols

Our Protocol consists of two sub–protocols: the *Merchant Registration Protocol* and the *Payment Protocol*. The main functions of both protocols are shown as follows:

Merchant Registration Protocol

$$
\begin{aligned}
&\mathbf{C} \rightarrow \mathbf{M}: \ \{NID_C, n, MIDReq, DCMAReq\}_w \\
&\mathbf{M} \rightarrow \mathbf{C}: \ \{ID_M, h(n, NID_C, ID_M)\}_w \\
&\mathbf{C} \rightarrow \mathbf{M}: \ \text{IF } (TS = \text{"}Kiosk\text{"}) \text{ THEN} \\
&\qquad\qquad \{n, MPReq\}_w \\
&\qquad\quad \text{ELSE} \\
&\qquad\qquad \{n, C_P\}_w \\
&\mathbf{M} \rightarrow \mathbf{C}: \ \text{IF } (TS = \text{"}Kiosk\text{"}) \text{ THEN} \\
&\qquad\qquad \{n, M_P, h(n, M_P)\}_w \\
&\qquad\quad \text{ELSE} \\
&\qquad\qquad \{n, C_P, h(n, C_P)\}_w
\end{aligned}
$$

As our protocol is designed to work on two different operational models, the first step is to determine in which one them the payment is going to take place. First, **C** assigns the value *Connected* to $DCCI$ if he/she is able to connect to internet from his/her mobile device. Then, **C** sends to **M** her nickname NID_C,