AMCIS 2000 Proceedings

Americas Conference on Information Systems (AMCIS)

2000

A Flexible Membership/Subscription Handling System in an e-commerce Environment

Charalampos Farmakis
University of Athens, farmak@di.uoa.gr

Dimitrios Stamoulis
University of Athens, dstamoulis@yahoo.com

Dracoulis Martakos
University of Athens, martakos@di.uoa.gr

Recommended Citation

Farmakis, Charalampos; Stamoulis, Dimitrios; and Martakos, Dracoulis, "A Flexible Membership/Subscription Handling System in an e-commerce Environment" (2000). *AMCIS 2000 Proceedings*. 28.
http://aisel.aisnet.org/amcis2000/28

A flexible membership/subscription handling system in an e-commerce environment

Charalampos Farmakis, Department of Informatics, University of Athens, farmak@di.uoa.gr
Dimitrios Stamoulis, Department of Informatics, University of Athens, dstamoulis@yahoo.com
Dracoulis Martakos, Department of Informatics, University of Athens, martakos@di.uoa.gr

Abstract

This paper addresses the authorization nature of a membership handling system over the Internet and an abstract architecture is presented, overcoming the drawbacks of mechanisms and techniques proposed and used so far. The system is based on Public Key Infrastructure utilizing attribute certificates.

Introduction

Social constructs become more complex in modern societies and a growing number of citizens become members of various organizations, groups, clubs, societies, associations etc. People subscribe to organizations that offer benefits to its members. Membership organizations sign agreements for preferential treatment of their subscribers. The subscribers/members have to carry with them the proof of their membership status and always be aware of how to make use of it in order to receive the special treatment arranged for them. It is somehow awkward to manage this complexity, as everyone’s wallet already accommodates a lot of membership cards, such as credit, pass-permit, membership-identity, benefit /loyalty cards.

In the physical world, a member has to hold an authorization instrument that is valid and must be aware of the benefits that each of the third party cooperating organizations (e.g. merchants) offer each time. When one has multiple memberships, it is hardly possible to remember which authorization instrument to use each time. Moreover, it is almost impossible for the membership organizations to instantly update its members for short-living, special offers. These inconveniences are caused because there is no mechanism to authorize the member on the spot and modify its membership status and rights.

In the virtual environment, the situation is even more complex. Internet users have to present their membership credentials to a merchant in order to purchase goods electronically at preferential rates. Besides the membership schemes of the physical world, Internet users form virtual communities (Armstrong and Hagel, 1996). Therefore, a need arises for authorization mechanisms over the Internet which are capable of handling multiple, complex memberships in an efficient and effective manner for the benefit of all the involved parties. Moreover, a membership handling system over the Internet should be more flexible and dynamic than its real world counterparts, in order to represent an advancement over the present situation of the physical world.

In this paper, the authorization nature of the membership handling problem is addressed and an abstract system architecture as a solution to this necessity is proposed, overcoming the drawbacks of mechanisms and techniques proposed and used so far (Lynch, 1997; Kaijser, P., et al., 1994; McMahon, 1995). The main difference between the existing mechanisms, which have been are designed for authorization rather than for membership/ subscription handling purposes, is the fact that user rights are managed centrally by the acceptor whereas, in the proposed system, the user privileges are managed by the membership organization - where they originally stem from. This is rather reasonable, because authorization schemes are designed to protect resources, whereas a membership/ subscription handling mechanism is designed to facilitate the effective use of membership rights for the benefit of all the involved parties, as identified below.

Requirements of a membership/ subscription handling system

In cases that subscriptions are part of an e-commerce transaction, four involved parties can be identified: the member/ subscriber, the membership organization, the mall/ shop and the bank. Each of them poses its own requirements for an effective membership handling system in an electronic commerce environment.

The subscriber/ member

Membership status should be updated on demand, so that the member need not remember the benefits s/he is entitled to.

Care-free shopping. Concerns about validation checks, e.g. expiration date, and about requesting the discount or benefit should not bother the member while shopping, due to his/her membership status.

Maximizing gains from multiple memberships. If a consumer participates to more than one membership organizations, then s/he should be able to choose the most convenient and beneficial membership scheme for him/her.

Security, anti-fraud protection. The authorization instrument should be valid for a short period of time. Thus, an intruder cannot use this authorization instrument to the same or to other malls for one’s own interest.

Privacy. The member presents the authorization instrument to the mall without necessarily enclosing personal information. The proof of his/her membership status is enough for the mall to grant access under special conditions to the requestor/purchaser. This feature implements the provision 2.1.5 of the AAA Authorization requirements specification (Farrell et al., 1999) stating that “AAA protocols must support the use of non-identifying information, e.g. to support role based access control”.

The membership organization

On-line, real-time management of memberships. The membership organization should be able to immediately suspend, grant, upgrade or degrade a membership status.

Modify the membership benefits policy dynamically. The membership organization should be able to modify immediately and at any time its benefits / loyalty schemes reflecting the changing agreements with the cooperating third parties, without being concerned about distributing and propagating them. This would also allow the membership organization to offer ‘last-minute’ opportunities for its members, which could not be otherwise communicated to the members, because they are valid for short periods of time.

The mall

Mechanism to identify customers having special rights. The mall must identify the authorization instrument of a customer in order to apply the rules, terms and conditions that the mall has agreed with the member’s organization. Therefore, it either has to own a subscription handling subsystem in, or to be associated with one. This is in accordance to the article 2.1.15 of the AAA authorization requirements specification (Farrell et al., 1999) stating that “AAA protocols may either be deployed independently or integrated with application entities”.

Updating membership benefits distribution. The membership handling subsystem of the mall has some sort of logic with which it accepts the authorization instrument and executes the requested transaction according to the rules pertaining to the membership status of the requestor. However, this logic that is embedded into membership handling subsystem of the mall is periodically updated to reflect the agreements between the membership organizations and the mall. This agreement described the special terms and conditions that the mall applies to the various membership schemes. Therefore, there must be a provision in a membership handling system for the aforementioned sort of communication to be initiated by either of the two parties. This requirement is also included into the AAA authorization requirements specification (Farrell et al., 1999). Article 2.1.12 says that: “AAA protocols must specify mechanisms for updating the rules which will be used to control authorization decisions”.

Security, anti-fraud protection. The authorization instrument is valid for one-use only. Therefore, the mall is protected from malicious replicas of an authorization instrument issued once.

The bank

Avoidance of total amount due calculations. The complexity of payment regarding the total payable price calculation should remain outside the bank’s payment systems. Banks prefer to receive payment orders ready for execution, without adding any further ado prior to the processing for clearing and settlement.

Existing membership handling methods

This section reviews a number of different methods that have been either used or proposed for subscription/ membership handling.

Access Control List

An access control list (ACL) is a list of identity - attribute pairs, maintained locally by merchants. When the consumer contacts the merchant, the merchant authenticates the consumer's identity (e.g. username/ password, consumer's IP address) and looks up his/her attributes in the ACL. Although ACLs are easy to implement, most of the requirements presented above cannot be fulfilled. The membership status cannot be modified by the membership organization in real time. Moreover, the ACL concept presumes that the merchant knows in advance all the potential relevant customer attributes, which yields to privacy problem.

X.509.v3 integrated certificates

The public key certificate format X.509 version 3 (Ford and Baum, 1997) can be used to combine arbitrary attribute-value pairs. Thus, multiple memberships can be integrated into one identity/ certificate.

This approach, however, has a number of drawbacks. Each membership organization has to communicate with the certificate issuer to construct a certificate with all the applicable attributes. However, there is no mechanism for selective presentation of attributes to the merchant. Moreover, since all the attributes are included into one certificate, the ability for dynamic modification of the membership status is limited.

SESAME PAC

SESAME project (Kaijser, P., et al., 1994; McMahon, 1995) has proposed extensions to Kerberos for membership handling. A consumer authenticates to Kerberos in the usual way, acquiring a Ticket Granting Ticket (TGT), which is used as a service ticket to contact the Privilege Attribute Server (PAS) for a proof of access rights in the form of a Privilege Attribute Certificate (PAC).

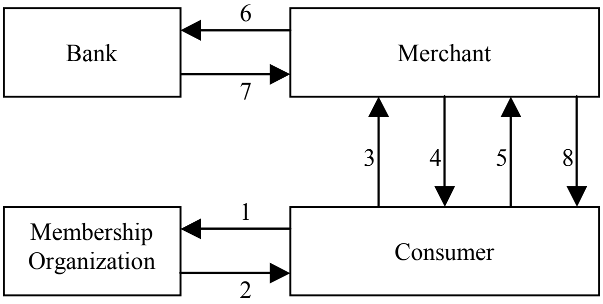
This centralized model assumes that many user memberships are known to the centralized Privilege Attribute Server, which limits the overall flexibility of the system. Moreover, multiple attributes in a PAC are exposed to each server.

Abstract system architecture and protocol

Based on Public Key Infrastructure, the abstract architecture of the system and the basic steps of the protocol are presented in Figure 1. Prior to any interaction amongst the parties involved, the following contractual relationships have to be in force: (a) the Consumer has a valid subscription with the membership organization, (b) the membership organization has a valid agreement with the merchant, for its users to have special rights, (c) the Consumer has the means to make a payment through the bank (e.g. an account) and (d) the Merchant has the means to receive the Consumer's payment through the bank.

In addition, it is assumed that the consumer knows what s/he wished to purchase - either via browsing at the merchant's site or through the membership organization and that s/he is aware about the special right available to him/her due to the membership. At this point, is should be noted that the consumer can be informed, at any time, about the benefits s/he is entitled to through the membership organization's information system, which also fulfills the "care-free shopping " requirement.

Figure 1: Abstract architecture



We use the notion "X → Y" to indicate that entity X sends a message to entity Y. We also use C to indicate the Consumer, O to indicate the organization at which the Consumer has a subscription, M to indicate the Merchant and B to indicate the Bank.

The basic steps of the protocol are the following:

(1) C → O Membership instrument request. The Consumer authenticates him/herself against the Membership Organization's information system and requests for an instrument that proves his/her membership.

(2) O → C The membership instrument is sent to the Consumer. It is an attribute certificate, which proves his/her membership to the organization. The membership instrument is valid for a certain, short, period of time, which protects both the merchant and the consumer from malicious use of this instrument over time. The fact that the consumer requests the authorization instrument shortly before it is used provides the ability for dynamic modification of the Organization's policy.

(3) C → M The membership instrument is forwarded to the Merchant's information system along with the request for the goods.

(4) M → C Membership instrument can be either accepted or rejected by the Merchant. In the first case, the Merchant responds asking for the payment instructions. If the membership instrument is not a valid one, an explanatory error message is sent to the Consumer and the session is terminated.

(5) C → M The Consumer responds with the payment instructions, which are encrypted with the Bank's public key and digitally signed with the Consumer's private key, ensuring that they are only visible to the Bank and cannot be altered.

(6) M → B The Payment instructions are forward by the Merchant to the Bank.

(7) B → M The Bank responds with the payment result, wither verifying the budget transfer or reporting an error.

(8) M → C If the payment instructions have been successfully executed, the goods are delivered to the Consumer. Otherwise, an explanatory error message is sent to the Consumer.

All messages exchanged between the involved parties are encrypted and digitally signed, in order to achieve integrity, confidentiality and non repudiation.

Conclusions

In this article we presented an abstract architecture and the relevant procedures that enable membership/ subscription handling over the Internet.

The authors are currently developing a communication protocol implementing the proposed abstract system architecture. The demo platform of a fully functioning membership handling system will be based on Baltimore's PKI plus Toolkit and will be developed in Java. The behaviour of this system will be tested in a real world case study (Papadopoulou et al., 2000) in order to finetune the communication protocol.

References

Armstrong, A. and Hagel J. “The real value of online communities”. *Harvard Business Review*, May – June '96, pp. 134-141.

Farrell, S. et al, "AAA Authorization Requirements", draft-ietf-aaa-authorization-reqs-01.txt, Oct. '99

Ford, W., and Baum S. "Secure Electronic Commerce", Prentice Hall, 1997, pp. 250-258.

Kaijser, P., et al., “SESAME: The solution to security for open distributed systems”, *Computer Communications*, (17:7), 1994, pp. 501-518

McMahon, P., “SESAME V2 Public Key and Authorization Extensions to Kerberos,” in Proceedings of the 1995 Symposium on Network and Distributed System Security, pp. 114-131, Feb., 1995.

Lynch, C. "A White paper on authentication and access management issues in cross-organizational use of networked information services", 1997, http://www.cni.org/projects/authentication/authentication-wp.html

Papadopoulou, P. et al., "A generic framework for the deployment of an Internet Billing Servicescape", Proceedings of the 21st Annual Business Conference, the 1st World Congress on the management of electronic commerce, Hamilton, Canada, January 2000.