

# A Privacy-Enhancing e-Business Model Based on Infomediaries

Dimitris Gritzalis<sup>1</sup>, Konstantinos Moulinos<sup>1,2</sup>, and Konstantinos Kostis<sup>1,3</sup>

<sup>1</sup>Dept. of Informatics Athens University of Economics & Business, 76 Patission Ave.,  
Athens, GR-10434 Greece  
{dgrit,kdm,kikigus}@aueb.gr

<sup>2</sup>Hellenic Data Protection Authority, Omirou 8 St., PC 10564, Greece

<sup>3</sup>Hellenic Army General Staff, Research and Information Systems Division/CCIS  
kostis@ccis.army.gr

**Abstract.** Rapid evolution of Internet may largely depend on gaining and maintaining the trust of users. This possibility may especially rule enterprises, whose financial viability depends on electronic commerce. Neither customers will have the time, the ability or the endurance to work out the best deals with vendors, nor will vendors have time to bargain with every customer. In order for customers to strike the best bargain with vendors, they need a privacy supporter, an information intermediary or infomediary. Infomediaries will become the custodians, agents, and brokers of customer personal information exchanged via Internet, while at the same time protecting their privacy. There is a scale between security and privacy that currently leans towards security; security adopts strong user authentication mechanisms in order to control access to personal data, while privacy requires loose authentication in order to provide user anonymity. In this paper we introduce a new infomediaries-based, privacy-enhancing business model, which is capable of providing anonymity, privacy and security, to customers and vendors of e-commerce. Using this model, customers of e-commerce can buy goods or services, without revealing their real identity or preferences to vendors, and vendors can sell or advertise goods or services without violating the privacy of their customers.

## 1 Introduction

The increasing popularity of Internet has generated significant interest in the development of electronic retail commerce. Internet has the potential to evolve into an interconnected marketplace, facilitating the exchange of a wide variety of products and services. Internet effects on the common commercial activities include, inter alia [1], by shifting power from sellers to buyers, by reducing the cost of switching suppliers and freely distributing a huge amount of price and product information. It also, reduces the transactions costs, the speed, range and accessibility of information,, the cost of distributing and capturing personal information, in order to create new commercial possibilities.

In order to identify customer preferences, and customize products and services, marketers are looking for new ways of capturing, processing and exchanging customer data. They collect data every time customers visit their web sites; they also

use numerous techniques to analyze that data and create mature user profiles. A user profile includes personal data, which may identify in a unique way a customer consuming behavior. Such a collection and processing of personal data may lead to private and family life violation, thus discouraging the public from using new technologies. According to a 1998 Harris poll, the lack of privacy and security in communications is the main reason of a consumer being off the Internet, and this is true for the great majority of potential users. Consumers are worrying about how their personal data will be used and how this data can be protected against unauthorized access [2].

A defense against online privacy infringement consists of business models and approaches that do not reveal the identity of the communicating parties. Such approaches are called anonymous. Internet operation may be based on anonymity. Should individuals wish to maintain the same level of privacy they enjoy in the real world, they should be given the choice for anonymity over the Internet.

Infomediarities (I/M) are business entities supporting the development of anonymous business models. Their basic role is to accumulate information about web users, and deal products and services on behalf of them. On the one hand, I/M can protect privacy by hindering marketers from collecting customer personal data, while they offer services, which maximize the value of a customer profiles. This paper presents such a business model, capable of supporting secure and anonymous electronic transactions. The use of I/M enable customers to increase their bargain capability without revealing personal data and, at the same time, enable vendors to promote products and services without violating customers' privacy. The paper is organized as follows: In section 2, a brief description of the privacy, anonymity and I/M notion is given, while in section 3 the major threats against digital trust and anonymity are presented. In section, 4 the existing privacy-enhancing technologies (PET) are presented. In section 5, the proposed model is presented. Section 6 refers to how most common threats are dealt with, by the proposed model. Finally, section 7 refers to the concluding remarks of the paper.

## 2 Definitions

Within the context of this paper *privacy* is the right of individuals, groups, or institutions to control, edit, manage, and delete information about them, and decide when, how, and to what extent that information may be communicated to others. On the other hand, *anonymity* is the ability of an individual to prevent others from linking his identity to his actions. Anonymity is examined as a service offered and ensured by communication networks. Confidentiality, as a service, is a means to offer privacy (usually by deploying encryption). The basic difference between confidentiality and privacy is related with the *subject* of information. Although information is confidential when the *owner* can control it, information is private when its *subject* can control it. Due to the fact that anonymous information has no subject, anonymity can ensure privacy. Confidentiality is the prerequisite for anonymity provision. An *Infomediatary* (I/M) is a business entity whose (sole or main) source of revenue derives from collecting consumer information, and developing detailed profiles of individual customers for use by selected third-party vendors [3]. I/M basic operation is based on matching customers consuming preferences with vendor products and services

offerings. In order to do so, customers send their preferences to I/M and the latter develop a customer personal profile. On the other hand, vendors send their offers to I/M, without establishing a direct communication channel with customers. The matching between customers preferences and vendors offers is compiled at I/M premises. Supposing that I/M are operating in a trusted environment, security and anonymity of customers' personal data are ensured.

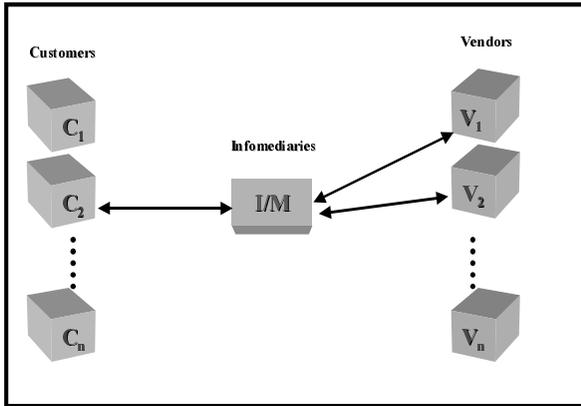


Fig. 1. Operation of infomediary

In a networked economy, customers' ability to collect information about their behavior and preferences implies that they can also choose to withhold this information from vendors. At the same time, the accessibility of such information has raised concerns about privacy. These characteristics of the new economic activities may lead to a status, where companies should have to negotiate with customers, should they wish to gain access to customer personal data. This process demonstrates the need of I/M that can handle negotiations and payments, and add value to customer personal information, while at the same time ensuring privacy [3,4]. The communication channels (Fig. 1) are vulnerable to various security and anonymity threats between the communicating parties. This is especially true when I/M are to operate in an insecure environment, such as the Internet.

### 3 Threats Against Security and Anonymity

A network of interconnected I/M is expected to evolve in a distributed global environment, such as Internet. Should an I/M gain customer trust, it has to be capable of defending against threats to digital trust and user anonymity. In the sequel, two categories of threats will be examined. Threats against *digital trust* in transit include [5,6]: Monitoring of communication lines, Shared key guessing, Shared key stealing, Unauthorized modification of information in transit, Forged Network Addresses, Masquerade, Unauthorized access, Repudiation of origin, Private key stealing and Private key compromise. Threats against *anonymous communication channels* include [7]: Message coding, Timing, Message volume, Flooding, Intersection and Collusion.

## 4 Privacy and Anonymity Supporting Technologies and Models

“Anonymous re-mailers” allow e-mail messages to be sent without revealing the identity of the sender. Some operate through Web pages where an e-mail is created and sent without any information identifying the sender. Other re-mailers are designed to receive an e-mail message from one party, re-address it and send it to a second party. In the process, header information that would identify the sender is removed [8]. They suffer by given disadvantages when it comes to implement a global e-commerce infrastructure. The basic drawbacks of remailers are: a) users must rely on the security of the operation site to resist intruders who would steal the identity table, b) attackers who could eavesdrop on Internet traffic could match up incoming and outgoing messages to learn the identity of the acronyms/pseudonyms and c) some remailers impose substantial delays and performance limitation.

*Rewebber* is a technology used for anonymous surfing the Internet. Firstly, a user visits the rewebber site and strokes the URL wishes to visit. Then rewebber manages, using various techniques, to substitute with another URL or encrypt the real URL. As a result the real communication channel between the requester address and the requested URL, is not revealed [9]. The basic disadvantage of this technology is that it often provides no protection against traffic analysis by means of timing attack, message volume attack, intersection attack, flooding attack, or collusion attack.

*TAZ servers* provide marketers with an easy way to point to potential consumers, as well as to offer consumers an easy way to access vendors. A TAZ server consists of a public database mapping virtual hostnames ending in *.taz* to re-webber locators. The database is public, so there is no incentive to threaten them with legal, social, or political pressure, because any information that the operator can access is also publicly available. A major disadvantage of TAZ servers is that a locator that contains a simple chain of rewebbers looks complicated; there is also a naming problem, still not solved [9].

*Onion Routing* [10] is a flexible communications protocol, resistant to eavesdropping and traffic analysis designed to provide anonymous, bi-directional and near real-time connections. The disadvantages of Onion routing are that it does not provide protection between end-users against timing attacks, message volume attacks (but only between onion routers), intersection attacks and flooding attacks.

*Crowds* [11] is a system for protecting user anonymity while browsing the web. It uses a strategy similar to Mixmaster and Onion Routing. Crowds operation is based on grouping users into a “crowd”. As a result, a user’s request to a web server is first passed to a random member of the crowd. That member can either submit the request directly to the end-server, or forward it to another randomly chosen member. In the latter case, the next member independently chooses to forward or submit the request. The disadvantages of Crowds are that it does not provide protection between end-users against timing attacks and message volume attacks, intersection attacks, or flooding attacks .

*JANUS* is a cryptographic engine that assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. JANUS is hiding the identity of recipients but not the identity of the senders [12].

*Web-Mixes* [7] is an anonymity system for the Internet. It uses a modified Mix [13] concept with an adaptive chop-and-slice algorithm, a ticket-based authentication system that makes flooding attacks impossible or very expensive, and a feedback

system giving the user information on his current level of protection. It also sends dummy messages whenever an active client has nothing to send. Web-mixes protects against coding attacks using public key cryptography, against timing and message volume attack using dummy traffic and chop-and-slice algorithm, but it provides no protection against intersection attack. It protects against flooding attacks by using “tickets”; it protects against collusion defending k-1 of k Web-Mixes.

The aforementioned technologies have the following disadvantages:

1. They provide encryption mechanisms as a means to provide anonymity, but fail to protect authenticity and integrity of the exchanged messages.
2. A subject enjoys privacy when he can control, on his own, the dissemination of his private information. These technologies exploit confidentiality mechanisms only to provide anonymity, but fail to control access to users personal data.
3. These technologies are more privacy-enhancing tools than models oriented to support global and anonymous e-commerce purchases. Thus, they do not integrate technologies, which help users explore and make use of the electronic marketplace.

## 5 A Privacy-Enhancing e-Business Model

Fig. 1 presents the basic operations of a single I/M. Additional functionalities should be described, should such a network of interconnected I/M emerge, operating in an untrusted environment. These functionalities include:

1. A secure acquaintance mechanism (e.g. I/M directory service) between different I/M. Thus, all new I/M members are capable of introducing themselves.
2. Users should trust I/M as they are agents of their personal information. Thus, a proper security infrastructure (i.e. I/M PKI) should be provided to implement this trust.
3. Integration of the basic I/M operations (i.e. customer profile creation, vendor offers collection, and matching) may violate users anonymity in case of collusion attack. In order to implement the “need to know” principle, these operations should be performed by different, independent, and special-purpose entities.

The suggested I/M model (Fig. 2) model takes into account the additional functionalities. It includes four distinct entities: the Customer, the Vendor, the Customer-oriented I/M and the Super-I/M (Table 1). For each entity there is a number of requirements and functionalities. The requirements refer to each entity expectations from the I/M PKI. The functionalities refer to the implemented functions, as well as to the roles played by each entity within the I/M PKI. Initially,  $C_x$ ,  $I/M_{cx}$ , and  $V_x$  have to register to  $I/M_S$  in order to join the PKI. A typical registration procedure may be followed using the web. At the end of this phase,  $I/M_S$  issues digital certificates identifying each party within the PKI.

The protocol used for the implementation of the suggested model is the following:

Case 1: Customer request:

1. Customer ( $C_x$ ) encrypts product description (PD) with the  $I/M_{cx}$  public key ( $P_{I/M_{cx}}$ ). Let  $M$  be the result of this procedure. Then, it sends a request to  $I/M_{sx}$ , containing personal information (P) and  $M$ , encrypted with  $I/M_s$  public key ( $P_{I/M_s}$ )

$$C \rightarrow I/M_s: \{P, M\}_{P_{I/M_s}}$$

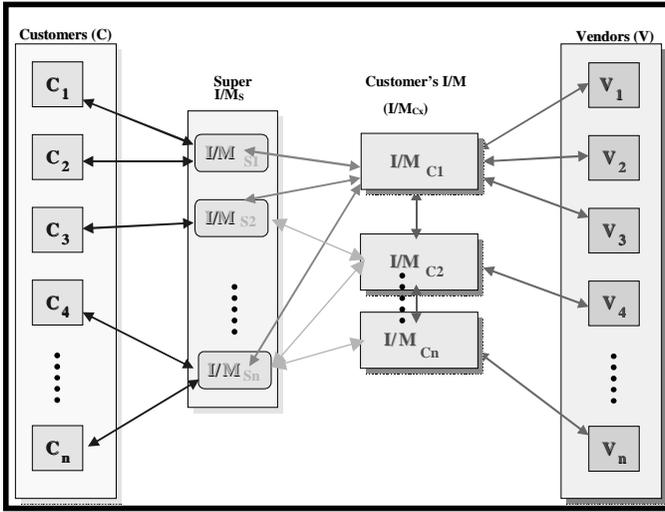


Fig. 1. The suggested model

Table 1. Model's entities, requirements, and functionalities

Entity	Requirements (expectations)	Functionality
Customer (C <sub>x</sub> )	Buy goods from vendors, Retain privacy and anonymity	
Vendor (V <sub>x</sub> )	Dispose products to customers, Increase their sales, Reduce the advertising cost, Gain more revenues, Aware of customers preferences	Delivery of products to I/M <sub>s</sub>
Customer oriented Infomediary (I/M <sub>Cx</sub> )	Act on customers' benefit, Own large databases, Increased marketing skills	Collection of product offerings, Building of profiles, Matching of profiles with vendors' products, Gathering of customers requests from I/M <sub>s</sub> , Reference to other I/M <sub>Cx</sub> when an I/M <sub>Cx</sub> request does not match an entry in the local database.
Super Infomediary (I/M <sub>s</sub> )	Trusted by vendors and customers	Supervision of model procedures, Setting up of the I/M PKI, Protection of anonymity, privacy, and authenticity, Collection of personal information, Collection of customer preferences

2. I/M<sub>s</sub> decrypts the received message using the private key corresponding to P<sub>I/Ms</sub>, anonymizes the information contained within C<sub>x</sub> request, substitutes P with a

random identifier (ID), and sends ID and  $M$  to  $I/M_{C_x}$  encrypted with the  $I/M_{C_x}$  public key ( $P_{I/M_{C_x}}$ ).

$$I/M_S \rightarrow I/M_{C_x}: \{ID, M\} P_{I/M_{C_x}}$$

- $I/M_{C_x}$  decrypts the received message using the secret key corresponding to  $P_{I/M_{C_x}}$ . Then, it decrypts  $M$  using the secret key corresponding to  $P_{I/M_{C_x}}$  and retrieves PD.

Case 2: Vendor offer:

- Vendor ( $V_x$ ) sends to  $I/M_{C_x}$  his personal random identification number (VID) accompanied with his product offer (PO), encrypted with  $I/M_{C_x}$  public key ( $P_{I/M_{C_x}}$ ).

$$V_x \rightarrow I/M_{C_x}: \{VID, PO\} P_{I/M_{C_x}}$$

- $I/M_{C_x}$  decrypts the received message using secret key corresponding to  $P_{I/M_{C_x}}$ , and appends VID and PO to its local database.

Case 3: Delivery:

- $C_x$  matches PD with PO (within the local database) and creates the response (R) corresponding to PD and accompanied with a response ID (RID). In case of an initial unsuccessful matching between PD and PO, a referral can be forwarded to another  $I/M_{C_x}$ . This procedure may be continued until initial request is satisfied, or a final matching failure is referred.

When a successful matching is performed, then  $C_x$  sends the following messages:

- 1.1 To  $V_x$ : It sends PD and RID encrypted with  $V_x$  public key ( $P_{V_x}$ ).

$$I/M_{C_x} \rightarrow V_x: \{RID, PD\} P_{V_x}$$

- 1.2 To  $I/M_S$ : It sends ID and RID encrypted with  $I/M_S$  public key ( $P_{I/M_S}$ )

$$I/M_{C_x} \rightarrow I/M_S: \{ID, RID\} P_{I/M_S}$$

- $V_x$  decrypts the received message (message 1.1) using the private key corresponding to  $P_{V_x}$ , and delivers goods to  $I/M_S$ .  $I/M_S$  decrypts the received message (message 1.2) using the private key corresponding to  $P_{I/M_S}$  and matches RID to P, through ID.
- When goods corresponding to RID delivered to  $I/M_S$ , it constructs a message containing ID, RID and send it to  $C_x$  encrypted with  $C_x$  public key ( $P_{C_x}$ ).
- $I/M_S \rightarrow C_x: \{ID, RID\} P_{C_x}$
- $C_x$  decrypts the message using the private key corresponding to  $P_{C_x}$ , retrieves RID corresponding to ID and is waiting for goods to be delivered.

The services, which are offered by I/M PKI are depicted in Table 2.

The new major element, which has been introduced by the suggested model, is the evolution of an I/M network operating in a trusted environment, as a means to protect customer privacy. The cornerstone of this model is the notion of an  $I/M_S$  supervising the operation of an I/M PKI. This element is introduced to increase privacy, anonymity, and security of customers.

An  $I/M_S$  can provide additional protection against collusion attacks. This kind of attacks can be exploited in case of direct communication between an  $I/M_{C_x}$ , which owns customers personal information, and  $V_x$ . An unscrupulous  $I/M_{C_x}$  could collate customer personal information with  $V_x$ 's database and thus violate customers' privacy. This can be avoided by stripping off customers' personal information by  $I/M_S$ . This way, neither customers, nor vendors, directly communicate to each other but through a trusted  $I/M_S$  clearing every transaction. Furthermore, product description request is hidden even from I/Ms by encrypting it with  $I/M_{C_x}$  public key. This way, no party

within I/M PKI can correlate identifiable personal information with customers' consuming behavior.

**Table 2.** Services offered by I/M PKI

<i>Service</i>	<i>I/M<sub>c</sub></i>	<i>I/M<sub>s</sub></i>
Registration		+
Key management		+
Cryptographic services		+
Digital Signatures		+
Non-repudiation (time-stamping)		+
Certificate management		+
Directory services	+	+
Camouflaging communications	+	+
User anonymity		+
Database management	+	+
Delivery		+

In order to avoid collusion attacks, personal information and matching operations are separated. According to the I/M model (Fig. 1), the acquaintance of customers personal information and its matching with a product offered by vendors is performed by the same entity. This may lead to collusion attacks if an I/M sells personal profiles to vendors. To avoid this, these operations have been assigned to different entities:

- Personal data collection is performed by a trusted organization (e.g. a Data Protection Authority). This organization anonymizes the personal data by substituting the person's identity with a randomly generated number. Each customer request is assigned a different id number. I/Ms know nothing about customer's consuming preferences because these preferences are encrypted with I/M<sub>Cx</sub>'s public key.
- I/M<sub>Cx</sub> performs the matching between anonymous customer preferences and vendor offerings. I/M<sub>Cx</sub> may be any company.

The use of a single I/MS, which supervises the I/M PKI, may lead to network traffic congestion problems. For this reason, a network of I/MS may be established. I/M<sub>Cx</sub> and V<sub>x</sub> registrations are now distributed between local I/MS. Furthermore, each I/M<sub>Cx</sub> occasionally communicates with its peers, in case matching referrals not appearing in its local database. To decrease network traffic payload, only changes to customers preferences and to vendors offerings database are transmitted. During the registration phase, I/MS and V<sub>x</sub> send the instances of their local databases to I/M<sub>Cx</sub>. From then on, only database instance changes are communicated with I/M<sub>Cx</sub>. Only asserted parties may be involved in the I/M PKI. Thus, every asserted entity should be equipped with a digital certificate. Directory services may be used in order for a I/M<sub>Cx</sub> to communicate with its peers and look up for a specific C<sub>x</sub> request not

satisfied by information included in its local database. Security of the model communication channels is achieved using digital certificates issued by I/MS during registration.

Two levels of end-to-end user anonymity may be distinguished:

(a) *Customers personal profile anonymity*, which refers to mechanisms adopted to protect personal data from revealing to unauthorized parties and it is achieved using the following mechanisms:

1.  $C_x$  communicates only with  $I/M_s$  who strips off the customer's personal information from his requests to  $I/M_{cx}$  by substituting P with ID (step 2 of communication protocol, customer request). This way no personal information is circulated within I/M PKI.
2. The intermediation of  $I/M_s$  during delivery of goods makes impossible the direct communication between  $C_x$  and  $V_x$ .

(b) *Communication level anonymity*, which refers to the mechanisms and technologies which may be adopted to camouflage communications among different parties. For communication level anonymity, Web-Mixes and Mix model mechanisms may be adopted. In detail, a chain of servers (Mixes-Chaum) can be used between  $C_x$  and  $I/M_{cx}$ . Each Mix in the chain strips off the identifying marks on incoming requests, and then sends the message to the next Mix, based on routing instruction which encrypted with its public key.  $C_x$  encrypts communication using the public keys of each Mix on the route. The Mixes store the requests (messages) they receive and - at designated intervals - randomly forward a request to its destination. If no message is waiting to be sent, then the Mix randomly generates a message to be sent.

Table 3 refers to the technologies and standards available for offering the services required by the suggested model.

## 6 How Common Threats Are Dealt with

Digital certificates and SSL protocol exploit public and symmetric key cryptography. These technologies are deployed to defend against most threats.

1. *Monitoring of communication lines*. Avoided by using Public Key Cryptography.
2. *Shared key guessing*. Avoided by using strong symmetric encryption.
3. *Shared key stealing*. Avoided by using public key encryption (protect transmission of shared keys in plaintext across a data network).
4. *Unauthorized modification of information in transit*. Avoided by using public key encryption during all communication steps between two parties.
5. *Forged Network Addresses and Masquerade*: We can distinguish two cases of forging:
  - An unscrupulous user pretends to be a self-signed  $I/M_s$ . This is avoided by issuing certificates by a trusted I/MS, only, and allow use within I/M PKI.
  - An unscrupulous user pretends to be a trusted party. Avoided by using certificate-hashing mechanisms.
6. *Unauthorized access*: Avoided through the use of a sound access control policy.
7. *Repudiation of origin*: Avoided by time-stamping all messages between  $I/M_s$  and other entities.

**Table 3.** Services and candidate technologies and standards

<i>Service</i>	<i>Candidate technologies</i>
Registration	WWW + SSL, SSH + custom application, Secure e-mail (S/MIME, PGP), Postal mail
Key management	ISO 8732, ISO 11770, PKCS
Cryptographic services	RSA Cryptokit, Microsoft CryptoAPI, Open Group GCS/API
Digital Signatures	ISO 9594, ISO 9796, ISO 14888, ISO 9798, GSS-API, Microsoft CryptoAPI, GCS API, PKCS
Non-repudiation (Time-stamping)	U.S Patent 5,136,647, Annex to ISO 13888-3, PKIX, ISO 13888
Certificate management	X.509, SPKI
Directory services	X.500/LDAP, Z.39.50
Camouflaging communications	Web-Mixes, Mix, Onion Routing
User anonymity	Request strip off
Database management	Medium-class or high-end DBMS supporting SQL
Delivery	S/MIME, PGP, Postal mail

8. *Private key stealing and Private key compromise:* Avoided by using strong encryption and by storing cryptographic tokens in removable media.
9. *Message coding.* Avoided by using end-to-end Onion Routing.
10. *Timing.* Avoided by using Mixes. A Mix waits until a defined number  $n$  of messages has arrived from  $n$  users. After that time, all messages are put out together, but in a different order. Also, dummy messages are sent from the starting point (i.e.  $V_x, C_x, I/M_{C_x}, I/M_s$ ) into the network to make traffic analysis harder. Large messages (and streaming data) are chopped into short pieces of a specific constant length ("slice"). Each slice is transmitted through an anonymous Mix channel. In addition, active users without an active communication request send dummy messages. Thus, nobody knows about the starting time and duration of a communication because all active users start and end their communications at the same time.
11. *Message volume.* Avoided by using Mixes. All incoming and outgoing messages of a Mix have the same length. To prevent replay attacks, a Mix will process each message only once.
12. *Flooding.* Avoided by using Mixes. Each user has to show that he is allowed to use the system at the respective time slice by providing a ticket valid for the certain slice, only. To protect the identity of the user the ticket is a blinded signature issued by the anonymous communication system.
13. *Intersection.* Use of dummy traffic makes intersection attacks harder but does not prevent them.
14. *Collusion.* Only  $I/M_s$  (trusted participant) issues digital certificates and public keys. In addition, the parties, which perform personal data collection and matching services, are different. Therefore, there is no way of direct communication neither between  $I/M_{C_x}$  and  $V_x$ , nor between  $C_x$  and  $V_x$ . As a second

level of prevention, customer's product description requests are encrypted with I/MCx's public key. This means that although I/Ms knows customer's personal information it cannot be correlated it with his consuming preferences. On the other hand, although I/MCx possess anonymous customer's consuming profiles, it cannot correlate them with any identifiable personal information. This way the "need to know" principle is enforced within I/M PKI.

## Conclusions

Exploiting Internet services usually means leaving personal digital traces. Anonymity and un-observability on the Internet is tough to ensure. On the other hand, there is a substantial need for anonymous communication, as a fundamental building block of privacy in the information society. Although existing technologies offer, more or less, serious technical advances with regard to communication camouflaging, they present substantial disadvantages when it comes to be adopted as global anonymous e-commerce carriers. On the other hand, infomediaries is a promising technology on the financial area, which has not been exploited on anonymous communication field. In this paper we have described a business model, based on the infomediaries concept, which is suitable for anonymity-aware and privacy-concerned users when making electronic purchases. The model allows users not to reveal their personal data or preferences to vendors, and at the same time allows vendors sell or advertise goods or services, without violating the privacy of their customers.

The basic characteristics of the suggested model are.

- The introduction of I/M as a privacy-enhancing agent in the e-commerce and e-government area. Although I/M have been mainly exploited as a means to establish new virtual enterprises and maximize user personal information value, they also offer new possibilities regarding privacy and anonymity.
- The stand-alone I/M model is neither adequate, nor security and anonymity robust for large-scale e-economies. Thus, the evolution of an I/M network, with entities co-operating in a secure and anonymous way, is introduced, offering anonymous electronic transactions.
- The traditional I/M model, which integrates customer preferences acquisition and vendor offerings, is vulnerable to collusion attacks. The separation of these operations is estimated to largely contribute in making anonymous global electronic purchases.
- Suggested model's candidate technologies are well established not only in the application level but also in the international standards area. This makes model's implementation feasible and compatible with existing privacy enhancing technologies. As a result, no further technical and operational turbulence will hesitate the integration of our model within e-commerce infrastructures.

Trust is a key element in e-commerce. If I/M are to play a role within the digital economy, they should limit the searching cost of goods and services. They should also help determining the best price for goods or services, support protecting the customer from unwanted intrusions by vendors, while at the same time support alerting a customer in case of new product offerings that meet his needs and preferences. Finally, they should ensure customers privacy and anonymity.

## References

1. Sarkar, Butler, Steinfield: Intermediaries and Cybermediaries: A Continuing Role for Mediating Players in the electronic marketplace. *Journal of Computer-Mediated Communication*, Vol. 1. **3** (December 1995)
2. Pfleeger C., Cooper, D.: Security and Privacy: Promising Advances. *IEEE Software Magazine*, Vol. 14. **5** (September/October 1997) 27–32
3. Hagel, Rayport: The new infomedaries. *The Mc Kinsey Quarterly*, **4** (November 1997)
4. Hagel, J., Singer, M.: *Net Worth: Shaping Markets When Customers Make the Rules*. HBS Press (1999)
5. De Vivo M., De Vivo G., Isern G.: Internet Security Attacks at the Basic Levels. *Operating Systems Review ACM press*, Vol. 32. **2** (April 1998) 4–15
6. Crijns, M., et. al.: Issues facing the secure link of Chambers of Commerce. European Commission, COSACC Project, Deliverable No. 3 (December 1998)
7. Berthold, O., Federrath, H., Köhntopp, M.: Project "Anonymity and Unobservability in the Internet"
8. Organization for Economic Co-operation and Development. Inventory Of Instruments and mechanisms contributing to the implementation and enforcement of the OECD privacy guidelines on global networks, DSTI/ICCP/REG(98)12/FINAL (19 May 1999)
9. Goldberg, Wagner: "TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the WWW". *First Monday Peer Reviewed Journal on The Internet*, Vol. 3. **4** (April 1998)
10. Cranor, L.: Internet Privacy. *Communications of the ACM*, Vol. 42. **2** (February 1999) 29–66
11. Reiter, M., Rubin, A.: *Crowds: Anonymity for Web Transactions – AT&T Labs Research*, [www.research.att.com/projects/crowds](http://www.research.att.com/projects/crowds)
12. Bleichenbacher, D., Gabber, E., Gibbons, P., Matias, Y., Mayer, A.: *On secure and Pseudonymous Client-Relationships with Multiple Servers* (May 1998)
13. Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms. *Com. of the ACM*, 24(2) (February 1981)