## Anonymous internet infrastructure based on pisa agents

Song, Ronggong; Korba, Larry



**Publisher's version / Version de l'éditeur:**
https://doi.org/10.4224/5763606
*Report (National Research Council of Canada. Radio and Electrical Engineering Division. ERB); no. ERB-1090, 2001*

National Research Council Canada
Conseil national de recherches Canada
Institute for Information Technology
Institut de Technologie de l'information

ERB-1090

NRC·CNRC

# *Anonymous Internet Infrastructure based on PISA Agents*

Ronggong Song and Larry Korba
November 2001

Canada

NRC 44899

National Research Council Canada
Institute for Information Technology

Conseil national de recherches Canada
Institut de Technologie de l'information

# *Anonymous Internet Infrastructure based on PISA Agents*

Ronggong Song and Larry Korba
November 2001

# Anonymous Internet Infrastructure Based on PISA Agents

Ronggong Song Larry Korba
Institute for Information Technology,
National Research Council of Canada
E-mail: {Ronggong.Song, Larry.Korba}@nrc.ca

**Abstract**

A vital requirement for e-commerce today is privacy. We explore the area of privacy for Agents in the Privacy Incorporated Software Agent (PISA) project. We first review existing privacy protection techniques: pseudonym systems, privacy enhancing technology (PET) and anonymous communication networks. We then propose a model for an Anonymous Internet Infrastructure (AII), an anonymous Internet based on PET-Agents, and analyze several possible combinations both of network technologies and PET-Agents. Finally, we discuss the security interface issues for PISA-Agents and present a pseudonym E-commerce model based on PISA.

## 1. Introduction

Privacy is becoming a critical issue on the Internet. Users feel that one of the most important barriers to using the Internet is the fear of having their privacy violated. Governments around the world have introduced legislation placing requirements upon the way in which personal information is handled. In attempt to provide some technical solutions within the privacy void, several network-based privacy-enhancing technologies have been developed in recent years. Some examples of these technologies include: Dc-Nets [10], JANUS proxy [5], MIX network [14, 38], Onion network [16, 33], Freedom network [39] and Pseudonym IP [51].

On the other hand, computers are commonly used for an increasing range of everyday activities. Generally, these activities are based on the exchange and acquisition of information. At present, however users, for the most part, still interactively and directly initiate all actions needed for a computer to perform tasks. With the use of software agents, actions may be executed with minimal supervision. This gives a user more time to spend on other activities. Recently, research and development efforts in the area of agent technologies have increased significantly. It is expected that agents will play an important role in the future information society and especially in e-business applications. Surprisingly, the research and development of these technologies is going on with little concern for the privacy issues raised by user demand and government regulations.

In [24] I. Goldberg gives an overview of existing and potential privacy enhancing technologies for the Internet. Based on the implementation techniques and functions, we can classify network-based privacy enhancing technologies into two kinds: one for converting user's identity into a pseudonym; and another is for hiding the user's identity, providing unobservability against traffic analysis via anonymous communication network techniques. Other privacy enhancing techniques include: information protection within agents, protection of agent code from intentional or accidental damage, secure distributed logs, among others.

In [4, 11, 20, 21, 29] several pseudonym techniques are proposed and developed. The primary goal of pseudonym techniques is to hide the user's identity using a pseudonym. Of course, pseudonym techniques have other advantages, e.g. authentication, abuse control, accountability, etc. Pseudonym techniques can be implemented using proxy or agent, etc. Actually, JANUS proxy belongs to this kind of techniques. Our PISA-Agent also belongs to this kind of techniques. The disadvantage of pseudonym techniques is that they cannot provide the personal data protection against traffic analysis by themselves. Traffic analysis protection is provided by anonymous communication networks.

In [1, 10, 14, 17, 19, 39, 44] some anonymous communication networks are proposed and developed. Current implementations of anonymous communication networks include Dc-Nets, MIX networks, Onion Routing networks, Crowds systems and Freedom networks. Pseudonym IP is only a proposal. The disadvantage of anonymous communication networks is that they cannot provide user's identity protection in the application data. This function should be provided with pseudonym techniques.

The PISA project involves the development of privacy enhancing technologies for next generation applications for electronic commerce. Distributed applications are foreseen as playing a major role in these next generation applications. Agent systems form one approach for distributed applications. Intercommunicating, multiple agents comprise multi-agent systems. They may communicate using a variety of different networks: wireless, wired; telephone, Internet, intranet, etc. These networks form the substrate upon which agent applications operate.

In this document, we provide an overview of the existing privacy protection techniques: pseudonym systems, PET and anonymous communication networks. In order to provide an advanced privacy protection technique, we propose a model for an Anonymous Internet Infrastructure (AII). AII offers an anonymous Internet based on PET-Agents. We analyze several probable combinations of both network technologies and PET-Agents. Finally, we discuss the security interface issues for PISA-Agents and present a pseudonym E-commerce model for PISA.

## 2. Background

What we wish to build is an anonymous Internet based on PET-Agents. An Anonymous Internet Infrastructure (AII) consists of the three components: pseudonym systems, PET-Agents, and anonymous communication networks over Internet.

***(1) Pseudonym Systems:***

A pseudonym system forms an important part of AII, and provides an information infrastructure for anonymous e-commerce applications. A pseudonym system consists of several entities such as certificate authorities, pseudonym and credential organizations, customers, etc.

***(2) PET-Agents:***

PET-Agents are directed toward providing anonymity of data content in agent-based e-commerce applications. They generate user's pseudonyms or credentials by converting identity into a pseudonym. In some situations (e.g. issuing pseudonyms or credentials), PET-Agents may be required to combine with pseudonym systems, or work as part of the pseudonym systems. In addition, PET-Agents have other functions like ISAT *(DEFINE ISAT)*.

***(3) Anonymous Communication Network:***

This is also an important part of AII. It provides an anonymous network preventing the capture of private information through eavesdropping and traffic analysis. In our AII, the pseudonym systems and PET-Agents should be interconnected through an anonymous communication network since they cannot provide this function on their own.

## 2.1 Pseudonym Systems

There is no question that Public Key Infrastructure (PKI) will play some role in the authentication of users, and components within e-commerce systems. But the current approach to digital certificate and PKI ignores the privacy rights of individuals, groups and organizations. Digital certificates can be followed, traced and linked instantaneously to individuals as they perform network-related activities.

Chaum first introduced pseudonym systems in 1985 [12], as a way of allowing a user to work effectively, but anonymously, with multiple organizations. Each organization may know a user by a different pseudonym, but these pseudonyms are not linkable: two organizations cannot combine their database to build up a dossier on the user. A user can obtain a credential from one organization using one of his pseudonyms, and demonstrate possession of the credential to another organization, without revealing his first pseudonym to the second organization.

In [4, 11, 20, 21, 29] some models for pseudonym systems are developed. In these models, a certification authority (CA) is needed only to enable a user to prove to an organization that his pseudonym actually corresponds to a public key of a real user. As well, there must be some stake in the secrecy of the corresponding secret key, such that the user can only share a credential issued to that pseudonym by sharing his secret key. As long as the CA does not refuse service, a cheating CA can do no harm other than introduce invalid users into the system.

Each user must first register with the CA, revealing his true identity and his public key, and demonstrating possession of the corresponding secret key, i.e. the user gets a public key identity certificate from the CA. After registration, the user contacts an organization and together they compute a pseudonym for the user. The user then may open accounts with many different organizations using different, unlinkable pseudonyms. However, all pseudonyms are related to each other—there exists an identity extractor that can compute a user's public and secret keys giving a rewindable user who can authenticate himself as the holder of the pseudonym.

An organization may issue a private credential to a user known by a pseudonym. A private credential may be single-use or multiple-use, and may also have an expiration date. Single-use private credentials are similar to electronic coins, since they can only be used once in an anonymous transaction. Some electronic coin protocols protect against double-spending by violating the anonymity of double-spenders, but generally do not protect against transfer of the coin. A private credential should be usable only by the user to whom it was issued.

The private credential has the following properties:

- ***Anonymity:*** Anonymity serves as the base case for privacy.

- ***Control:*** In many situations, full anonymity is not beneficial to anyone. Importantly, often at least one of the parties in a transaction has a legitimate need to verify previous contacts, the affiliation of the other party to a group, the authenticity of personal data of the other party, the eligibility of the other party to perform certain actions, and so on.

- ***Credential Sharing Implies Secret Key Sharing:*** A user who has valid credentials might want to help his/her friend to obtain whatever privileges the credential brings improperly. He/she could do so by revealing his/her secret key to his/her friend, so that his/her friend could successfully impersonate his/her regards.

- ***Unlinkability of Pseudonyms:*** Untraceability of an isolated transaction is not sufficient to prevent linking of different transactions that originate from the same individual. Without unlinkability, all an individual's past and future transactions become traceable as soon as the individual is identified in a single one of these. Without unlinkability, individuals cannot control how much data they actually disclose.

- ***Unforgeability of Credentials:*** A credential may not be issued to a user without the organization's cooperation.

- ***Selective Disclosure:*** The holder of private credentials can show the private credentials' attributes without revealing any other information about the private credentials.

- ***Reissuance:*** In many cases one's right to access a service comes from a pre-existing relationship in which identity has already been established. The CA can refresh a previously issued private credential without knowing the attributes it contains. The attributes can even be updated before the private credential is recertified.

- ***Dossier-Resistance:*** A private credential can be presented to an organization in such a manner that the organization is left with no mathematical evidence at all of the transaction. This is like waving a passport when passing customs. Alternatively, a private credential can be shown in such a manner that the verifier is left with self-authenticating evidence of a message or a part of the disclosed property.

- ***Pseudonym as a Public Key for Signatures and Encryption:*** Additionally, there is an optional feature of a pseudonym system: the ability to sign with one's pseudonym, as well as encrypt and decrypt messages.

Privacy protection requires that each individual has the power to decide how his/her personal data is collected and used, how it is modified, and to what extent it can be linked. Only in this way can individuals remain in control over their personal data. When using private credentials, organizations cannot learn more about a private credential holder than what he/she voluntarily and knowingly discloses, even if they conspire and have access to unlimited computing resources. Individuals can ensure the validity, timeliness and relevance of their data.

Private credentials are beneficial in any authentication-based environment in which there is no strict need to identify individuals at each and every occasion. Private credentials do more than protect privacy: they minimize the risk of identity fraud.

More generally, private credentials are not complementary to identity certificates, but encompass them as a special case. Thus, pseudonym systems can subsume systems based on identity certificates.

Pseudonym systems are very useful, especially in electronic commerce environment. The reason is that the accountability and anonymity are essential properties for fair exchange in e-commerce transaction. Clearly, anonymity is intended to hide a user's identity, whereas accountability is intended to expose the user's

identity, thereby holding the user responsible for his/her activities. The Pseudonym system is an effective solution technique for that. Pseudonym techniques can be implemented using client-side proxy, server-side proxy or intermediate agent. Actually, JANUS is a client-side proxy, and PET-Agent is an intermediate agent.

Private credentials by themselves do not protect against wiretapping and traffic analysis. On networks such as the Internet, one can transmit from a computer that is part of a network located behind a firewall, deploy pseudonymous services such as MIX network, Onion Routing network or Freedom network.

## 2.2 Private Incorporated Software Agent (PISA)

### 2.2.1 Identity Protector

In [26, 41] the identity protector (IP) techniques are discussed to protect the privacy of the user. The identity protector can be seen as a system element that controls the exchange of the identity between the various system elements. An important function of the identity protector is the conversion of a user's identity into a pseudonym. The pseudonym is an alternate (digital) identity that the user adopt when using the system. Examples of pseudonyms in conventional information systems include account numbers at banks and social security numbers for the tax authorities. In the conventional and future information systems, the identity protector may take the form of, say, a separate functionality within the information system.

The identity protector is installed on one of the interaction lines in the information system. This means the user's identity can no longer be spread to the cordoned off area of the information system. The identity protector protects the interests of the user -- specifically, it screens dissemination of his identity. Just as the service-provider wishes to protect his services, the user wishes to protect his identity.

As J..Borking's description, the identity protector offers the following functions:
- It reports and controls instances when identity is revealed;
- It generates pseudonyms;
- It translates pseudonyms into identities and vice versa;
- It converts pseudonyms into other pseudonyms;
- It combats misuse.

The user can set the identity protector for certain purposes. For example, his identity can be kept entirely confidential when the system is used legitimately. Another possibility is for the user to set the identity protector to reveal his identity only to certain service-providers. An identity protector creates two domains within the information system: "identity domain" and "pseudo-domain". The "identity domain" denotes the domain in which the user's identity is known, the domain in which the user's identity is secret are termed "pseudo-domain" (see figure 1).

The user must be able to trust the way his personal data is handled in the domain where his identity is known. The identity protector can be placed anywhere in the system where personal data is exchanged. This offers some solutions for privacy-compliant information systems. Techniques that can be used to implement an identity protector are: digital signatures, blind digital signatures, digital pseudonyms, and trusted third parties.

Depending on the elements within the information system that can be trusted, a number of configurations of a privacy information system can be distinguished, in which the user's identity is unlinked from parts of the information system as the following descriptions.

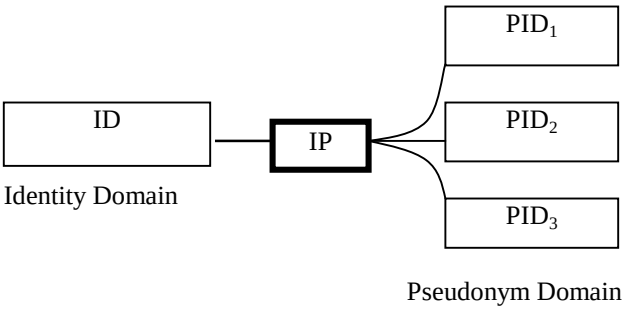


Figure 1. The identity protector separates the identity and pseudo domains

***(1) Protection of services***

The service elements of an information system can be structured in such as a way that the privacy of the user is not adequately protected. By placing identity protectors between the services and the other elements of the information system, privacy protection can be improved.

This means services are located in the pseudo-domain, while other elements remain in the identity domain (see figure 2). When an identity protector is integrated into a system, the user can use services anonymously, not only increasing privacy in terms of that particular service, but in relation to other users.

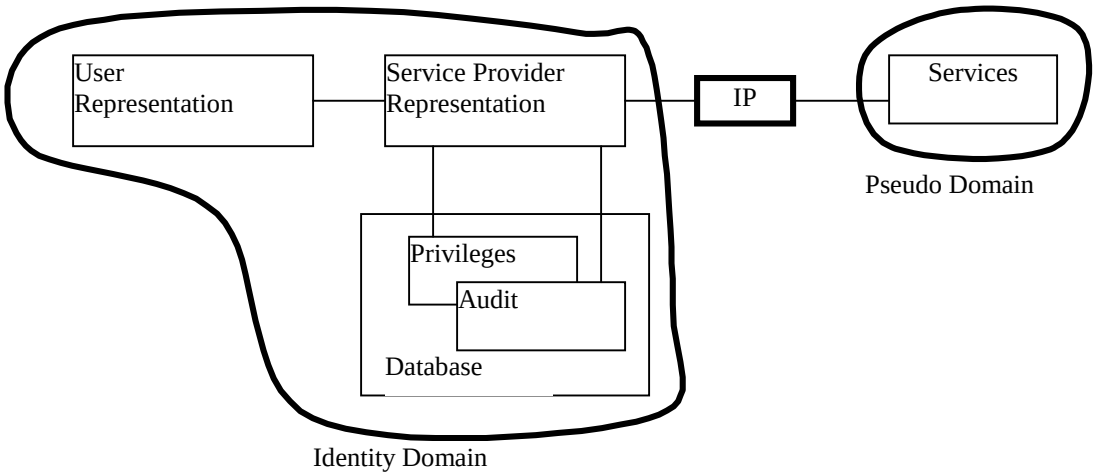


Figure 2. An identity protector protects the privacy of a service user

***(2) Protection of registration in the database***

A service-provider's database consists of a privileges file and an audit file. The privileges file contains the users' privileges and the audit file contains all the other information the service provider has recorded for provision of his services. Since these two files may register personal data, this system element merits the special attention of the privacy-conscious designer. The identity protector makes the designer minimize the

personal data filed in the database. The service-provider does not register the user's privileges and actions under his real identity, but under a pseudonym. Figure 3 depicts a situation in which both the privileges file and the audit file are included in the pseudo-domain.

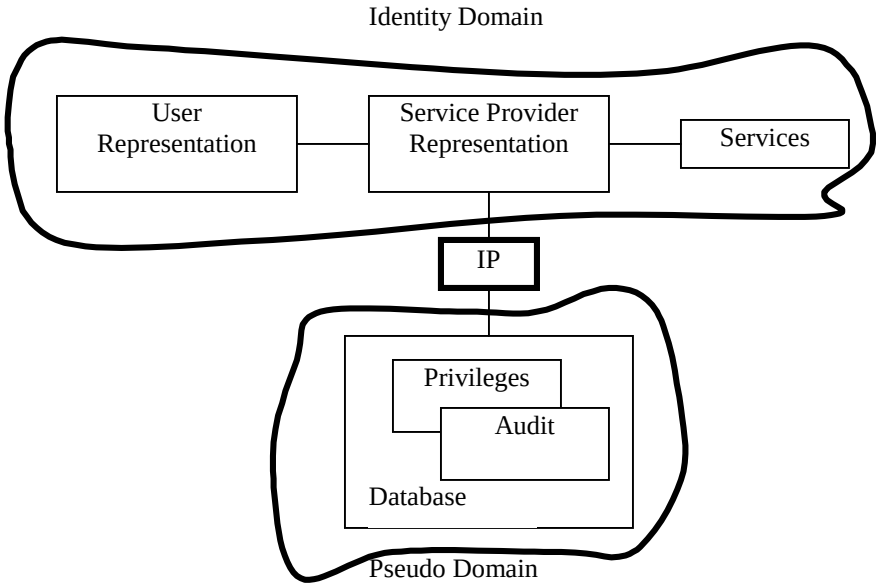


Figure 3. An identity protector prevents the registration of the user's real identity.

***(3) Protection of the entire information system***

In this situation, the identity domain only contains the user representation. By placing the identity protector between the user representation and that of the service-provider, a pseudo-domain emerges which envelops the services, service-provider's database, and the service-provider representation itself.

An important aspect of this configuration is that the service-provider must be able to determine what the user is authorized to do, without learning the user's identity.

Within the configuration, the identity protector acts as a sort of intermediary for the processes both the user and service-provider go through. So both parties must be able to trust the identity protector. Techniques that are suitable for use with a "trusted third party" are also suitable for an identity protector in this situation.

### 2.2.2 PET-Agents

To manage private threats, all security technologies (e.g. Identity Protector), applied in such a way that they can improve the privacy of individuals, are called Private Enhancing Technologies (PETs). PET-Agent is the integration of these PETs into the core of the Intelligent Software Agent Technologies (ISATs), the goal of the Privacy Incorporated Software Agent (PISA) project.

This topic is not dealt with in this investigation since it is the domain of work packages in PISA. Refer to those work packages for a description of available technologies (http://pet-pisa.openspace.nl/).

Like pseudonym systems, PET-Agents by themselves do not protect against traffic flow analysis. It would be best to combine PET-Agents with an anonymous communication network, such as MIX network, Onion Routing network, Freedom network or others.

### 2.3 Anonymous Communication Network

The primary goal of the anonymous communication network is to protect user anonymous communication against traffic analysis. In [19] D.R.Simon proposes a formal model of an anonymous communication network in 1996. It is assumed that parties can communicate anonymously. In the simplest of such models, parties can send individual messages to each other anonymously. A stronger assumption is that parties receiving anonymous messages can also reply to them; an intermediate one is that one or more parties can broadcast messages efficiently and thus reply to anonymous ones without jeopardizing that anonymity. But Simon's model assumes that reliable, synchronous communication is possible. While this simplifying assumption may be unrealistic, it is not actually exploited in his proposed protocol. Rather, the assumption of synchrony serves to discretize time, abstracting out the issue of communications delays without preventing adversaries from taking advantages of them since messages arriving during the same time period are queued in arbitrary order, as if any of them might have arrived first.

This assumption of anonymous communication has actually been studied fairly extensively, for example, MIX network in [14] and Dc-Nets in [10]. Based on Chaum's MIX networks, Wei Dai has described a theoretical architecture that would provide private protection against traffic analysis based on a distributed system of anonymizing packet forwarders. He called it Pipenet [44]. Pipenet consists of a cloud of packet forwarding nodes distributed around the Internet; packets from a client would be multiply encrypted and flow through a chain of these nodes. Pipenet is an idealized architecture and has never been built. Pipenet's mortal disadvantage is that its packet loss or delay is extremely large.

Like Pipenet architecture, in [16, 17] an Onion Routing network has been proposed and provides a more mature implementation to protect user anonymity against traffic analysis. With Onion Routing, a user directs his applications to contact application proxies that form the entrance to the cloud of nodes. The application proxy will then send an onion packet through a string of Onion Routers in order to create a route through the cloud. The application proxy will then forward the application data along this route through the cloud, to exit on the other side, and be delivered to the server to which the user wishes to connect. Onion Routing has no support for pseudonymity.

Freedom network [1, 39] is another similar technique for protecting user anonymity against eavesdropping and traffic analysis. It provides unobservable and anonymous real-time connections between network nodes. It works in a very similar way to the service Onion Routing network. Its advantage is that the data must only be encrypted or decrypted via a symmetrical cryptographic system. All data transmitted over one route are linkable.

In [50] O.Boucher, H.Federrath and M.Kohntopp propose a perfect anonymous communication system. In their approach, there cannot occur a situation where an opponent gets valuable information concerning any communication relation or communication request from and to a certain user. However, they assume that the opponent may not be able to break into cryptographic functions because no system can protect from an opponent with unlimited power. The perfect anonymous communication system should prevent the following attacks:

- ***Collusion Attack:*** A corrupt coalition of users or parties of the system may be able to trace certain users. Thus, an idea anonymous communication system would be a distributed system.

- ***Message Coding Attack:*** If messages do not change their coding during transmission they can be linked or traced. Thus, the sender should encrypt the message using nested layers of encryption in an ideal system. Each node removes one layer.
- ***Message Volume Attack:*** The amount of data transmitted between entities can be observed. A global observer is able to associate a communication relationship between peers or certain clients and servers. Thus, all incoming messages to a node should have the same length in a perfect system. All outgoing messages from a node also should have the same length.
- ***Timing Attack:*** An opponent can observe the duration of a specific communication by linking its possible endpoints and waiting for a correlation between the creation and release event at each possible endpoint. Thus, if the aim is protecting real-time services, dummy messages should be transmitted in order to reduce delay.
- ***Flooding Attack:*** Each message can only be anonymous in a group of sent messages. All servers of those messages form the anonymity group. Each sender should send one message per time interval. However, an attacker may flood the system in order to separate certain messages. It is very difficult to prevent flooding attacks in the Internet. One solution is to use authentication, via the use of "tickets".
- ***Intersection Attack:*** An attacker may trace users by observation over a long period. It is a well known open problem and seems extremely difficult to solve in an efficient manner.

Based on whether the network provides real-time communication or not, anonymous communication networks can be divided into two classes: store-and-forward and interactive anonymous communication networks.

- ***Store-and-forward anonymous communication networks:*** In these networks, the sender transmits his messages, and perhaps after some time, it arrives at the recipient. MIX network belongs to this kind of anonymous communication networks.
- ***Interactive anonymous communication networks:*** In these networks, the sender and recipient are communicating in real time. Large delays are not acceptable between transmission and reception of messages. These kinds of anonymous communication networks include Onion Routing network, Freedom network, Crowds system, NymIP. These networks have critical requirements on delay because the low-latency requirement can often introduce timing correlations that an eavesdropper can use to defeat the privacy of the system.

Anonymous communication networks offer the ability of hiding some metadata of Internet communication, but anonymous communication networks by themselves do not provide anonymity of data content because they do not deal with data content in any way. However, some applications insert information identifying the client to the application data itself. In terms of the PISA project, a PET-agent can be used to remove all identifying information from any application data that is about to be sent over the anonymous communication networks to prevent this exposure.

## 3. AII Model Based on PISA

In our AII, based on identity protector's position in an agent-based environment (Figure 4), we divide AII Model into two models: AII Model I and AII Model II. The AII Model I is intended for the situation where the identity protector is placed between the Agent and the external environment. In this model, the identity protector is for the protection of services (see Figure 2). The agent-provider has comprehensive powers to obtain and record personal data from its user. Thus, PET-Agent must be a trusted entity.

The AII Model II is intended for the situation where the identity protector is placed between the user and the Agent. In this model, the identity is meant to protect the entire information system. There are two methods for the implementation of the identity protector. One is installing a client-side identity protector proxy in the user's machine. It may be difficult for the agent-provider to determine what the user is authorized to do, without learning the user's identity. In order to make this question simple, another method is where the identity protector acts as a "trusted third party" for the processes both the user and agent-provider go through. We call the trusted third party as $PISA_{TTP}$. Of course, both parties must form a trust relationship with the $PISA_{TTP}$.

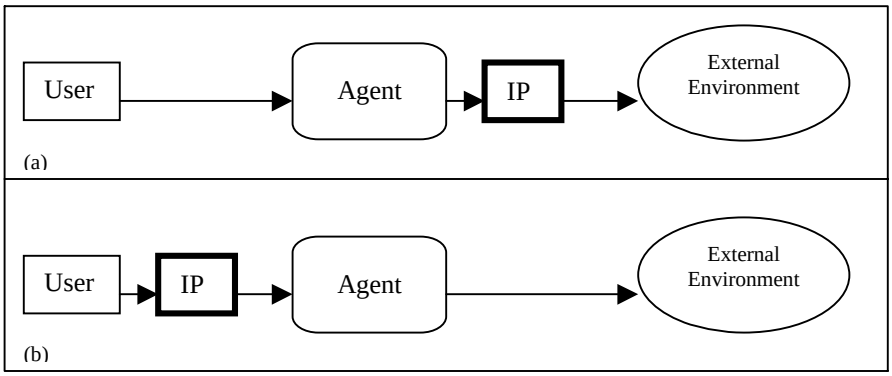


Figure 4. The identity protector placed in an agent-based environment.

### 3.1 AII Model I Based on PISA

In this model, the identity protector is placed between the Agent and the external environment. Thus, the PET-Agent has comprehensive powers to obtain and record personal data from its user. The identity protector will help the PET-Agent protect the personal data of its user against unwanted dispersion. In this situation, we suppose that the PET-Agent is operating in a trusted environment, security and anonymity of user's personal data are ensured.

The PET-Agent's basic operation is based on matching a user's profile with available functions. For example in a labor market environment, users first register using their identity and password, and then send their personal information including their history, abilities, skills, labor history etc. to the PET-Agent. The PET-Agent develops the user's personal profile. On the other hand, the PET-Agent gets the position descriptions from companies and organizations, and stores the information in its database. The PET-Agent then makes a match between the user profile and the demands of the party requiring personal. Or the PET-Agent may need to take the user's profile to the other PET-Agent. So in this matching process the personal data should be exchanged in an anonymous way.

Based on the different network environments that the PET-Agent may operate, the AII Model I has three different configurations, i.e. over a normal Internet, a large intranet and an anonymous communication network.

- ***Over normal Internet:*** If the PET-Agent operates over the normal Internet, an end-to-end authentication, integrity and encryption connection between the user and the PET-Agent is required. An end-to-end authentication and integrity connection between the PET-Agent and the vender is required. These security

mechanisms can be provided with IPSEC, TLS, OPENPGP, etc. Figure 5 depicts this configuration, where C means customer, V means vender, ID means identity, and PID means pseudonym identity. The disadvantage of this configuration is that it cannot provide anonymous protection against traffic analysis.

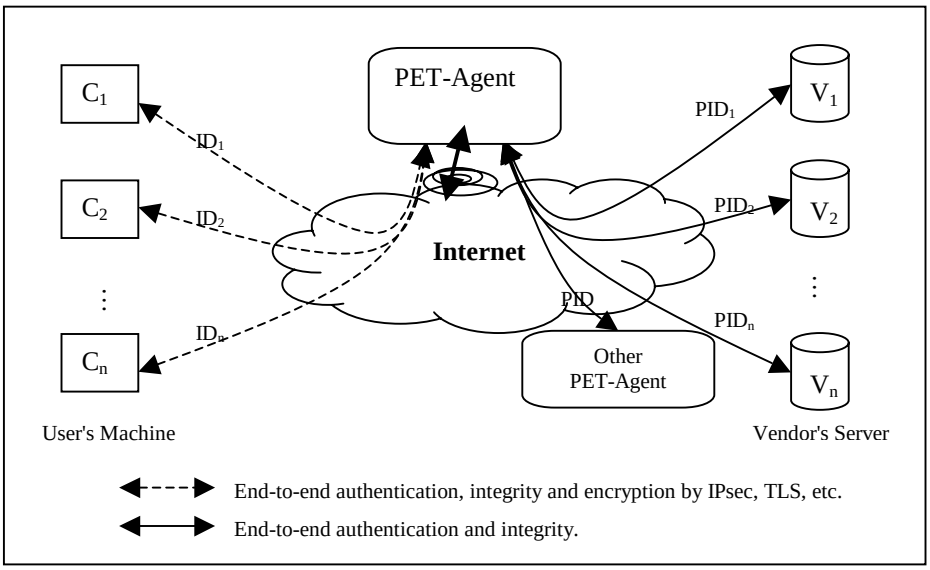


Figure 5. AII Model I over the normal Internet.

In this kind of configuration model, if the users are placed in a large intranet and behind a firewall, it can provide personal data protection against traffic analysis in some ways.

- ***Over a large intranet:*** If the PET-Agent operates over a large intranet, an end-to-end authentication, integrity and encryption connection between the user and the PET-Agent may be required. If the user is a remote access user (e.g. by dial-up or wireless), the end-to-end security can be provided with RADIUS Protocol, AAA, etc. An end-to-end authentication and integrity connection between the PET-Agent and the vender is required. These security mechanisms can also be provided with IPsec, TLSTLS, openPGP, etc. Figure 6 depicts this configuration.

  The advantage of this configuration is that it can provide anonymous protection against traffic analysis from the Internet in some ways. But it still cannot provide anonymous protection again traffic analysis from local attackers.

  In addition, the PET-Agent is placed in the client-side intranet in the above configuration. If the PET-Agent is placed in the vendor-side intranet and the users access the PET-Agent through Internet, this kind of configuration still cannot provide anonymous protection against traffic analysis.

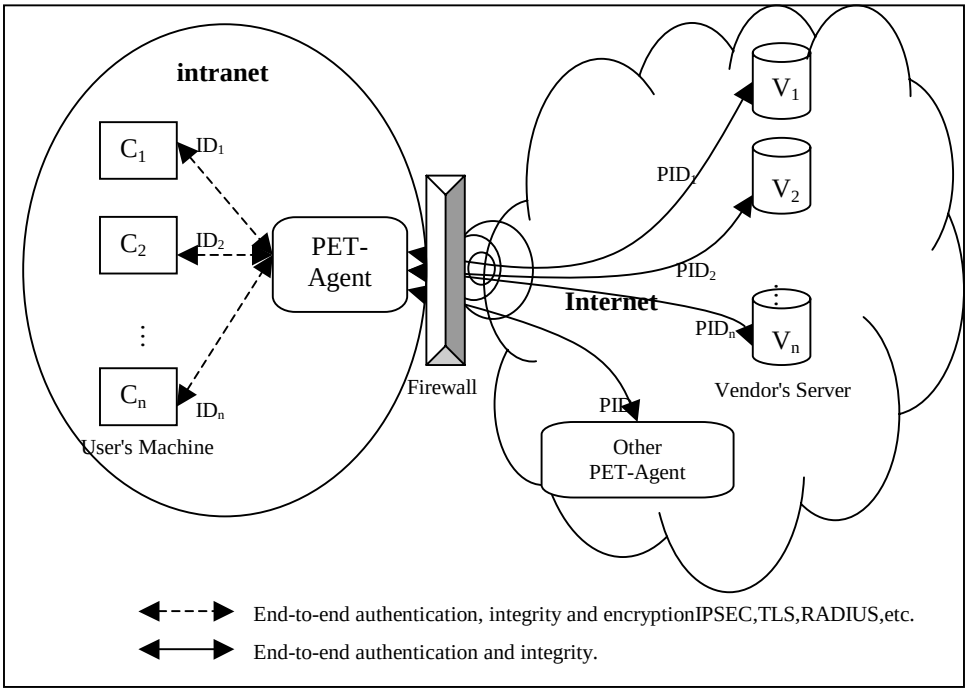


Figure 6. AII Model I over a large intranet.

- ***Over anonymous communication network:*** Like the configuration over the normal Internet, the end-to-end security between the user and the PET-Agent and between the PET-Agent and the vender is still required. These security mechanisms can be provided with IPsec, TLS, PGP, etc. Figure 7 depicts this configuration. The advantage of this configuration is that it can provide stronger anonymous protection against traffic analysis.

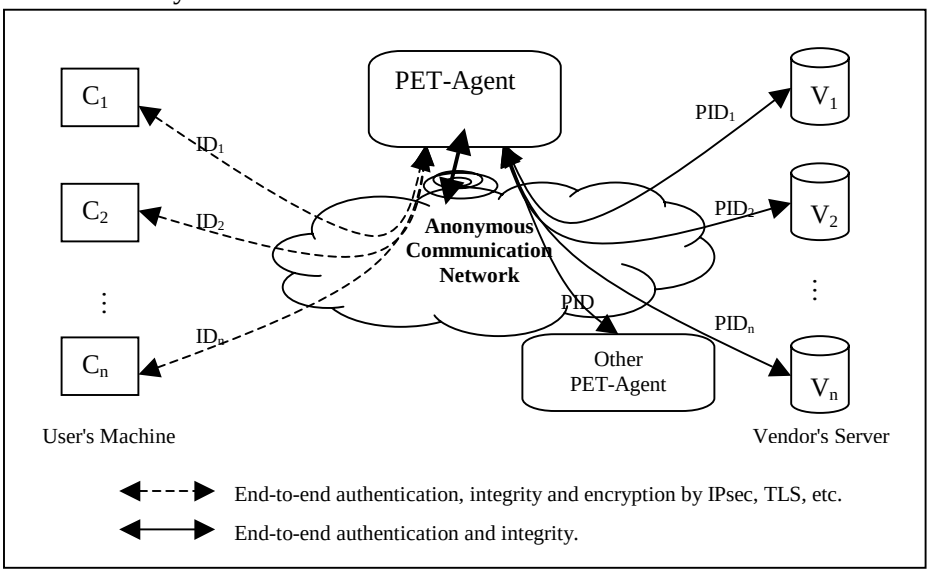


Figure 7. AII Model I over an anonymous network.

The disadvantage of the AII Model I is that it cannot be used to protect the user against threats to privacy caused by the agent-provider.

Other issues associated with the approaches described above are those of scalability and reliability. Rather than a single PET-Agent, many of them would be deployed, sharing the responsibilities for identity protection. This would limit the exposure of having a single point of contact for PET services, and increase throughput via resource sharing. We have not yet investigated how PET-Agents would be deployed to optimize scalability and reliability. These will be dealt with in later in this work.

### 3.2 AII Model II Based on PISA

In the AII Model II, the identity protector is placed between the user and the PET-Agent. Thus, there will be no exchange of personal data from the user to the agent without the approval of the identity protector and the user. In this way, the user can control the amount of personal data recorded by the PET-Agent. This option can be used to solve the threats caused by agent-provider in the AII Model I.

As the mentioned above, there are two methods for implementing the identity protector. One is using a client-side identity protector proxy. Another is using a third trusted party: $PISA_{TTP}$. Their purpose is to convert all identity information into pseudonym identity information appeared in any application data.

When using the client-side proxy, the user first needs to apply some pseudonyms or credentials from the pseudonym systems or the PET-Agent. He/she then registers using his/her pseudonym or credential, and send his/her profile with pseudonym to the PET-Agent. If using the $PISA_{TTP}$, the communication between the user and the PET-Agent must go through the $PISA_{TTP}$. The $PISA_{TTP}$ is a trusted entity by the users and the PET-Agents.

Like the AII Model I, the AII Model II also has three kinds of configurations, i.e. over a normal Internet, a large intranet and an anonymous communication network.

- ***Over normal Internet:*** Like the AII Model I, if the user uses a client-side proxy for identity protection, end-to-end security between the user and the PET-Agent and between the PET-Agent and the vender is still required. These security mechanisms can be provided with IPsec, TLS, PGP, etc. Figure 8 depicts this configuration.

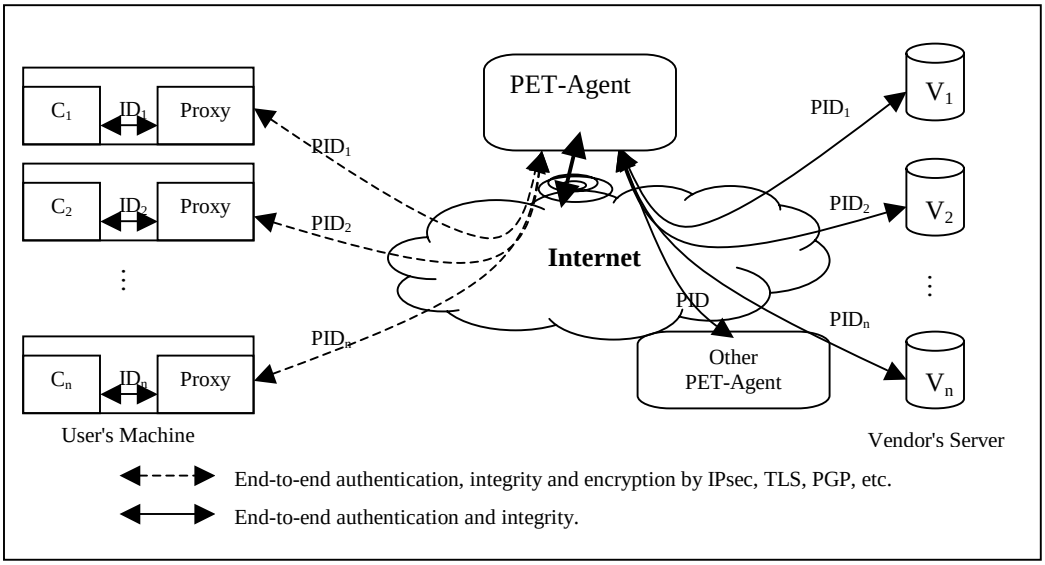


Figure 8. AII Model II over the normal Internet with proxy.

Another configuration is for the user to use the $PISA_{TTP}$ as the identity protector. An end-to-end security between the user and the $PISA_{TTP}$, between the $PISA_{TTP}$ and the PET-Agent, between the PET-Agent and the venders is required. They can be provided with IPsec, TLS, openPGP, etc. Figure 9 depicts this configuration.

Like the first configuration in the AII Model I, these configurations cannot provide anonymous protection against traffic analysis. But if the users are placed in a large intranet and behind a firewall, it can provide a certain amount of personal data protection against traffic analysis.

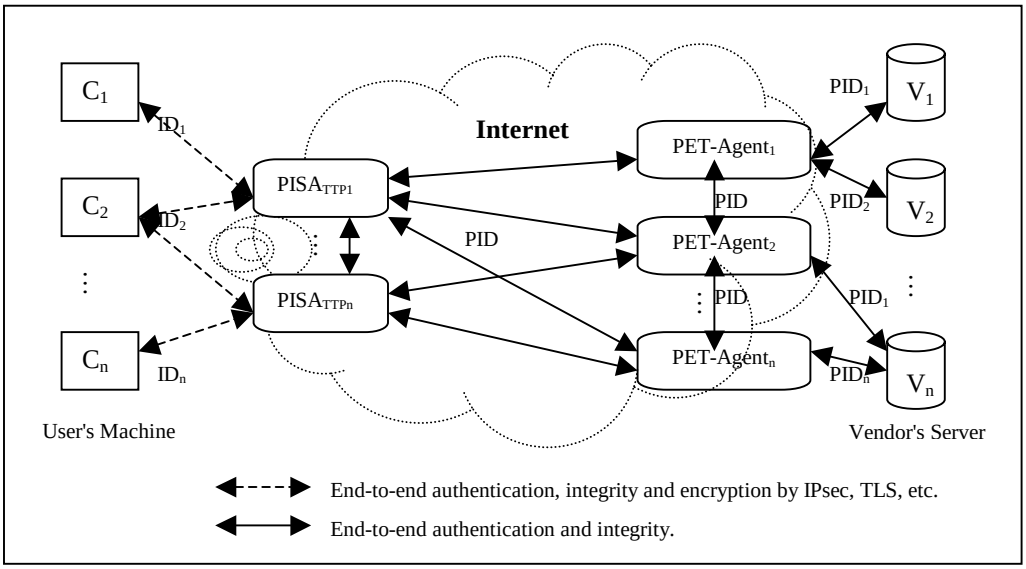


Figure 9. AII Model II over the normal Internet with $PISA_{TTP}$.

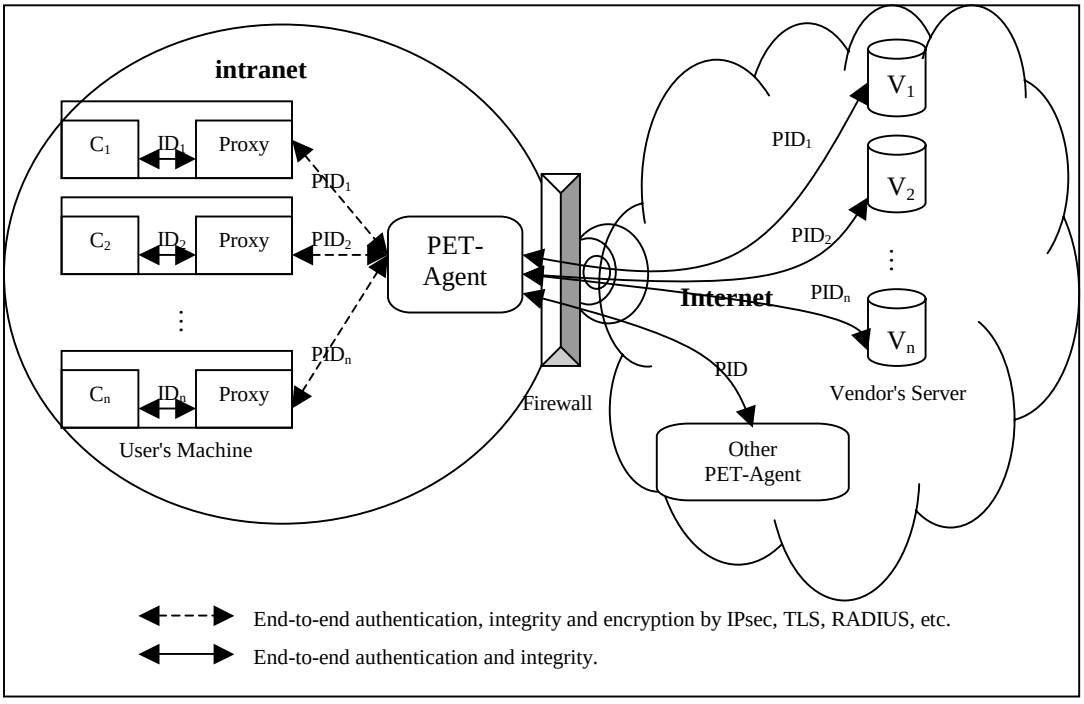


Figure 10. AII Model II over a large intranet.

- ***Over large intranet:*** Like the second configuration in the AII Model I, end-to-end security between the user and the PET-Agent is still required. If the user is a remote access user (e.g. by dial-up or wireless), the end-to-end security can be provided with Radius Protocol, AAA, etc. An end-to-end security between the PET-Agent and the vender is required. These security mechanisms can also be provided with IPsec, TLS, openPGP, etc. Figure 10 depicts this configuration. The advantage of this configuration is that it can provide anonymous protection against traffic analysis in some ways.

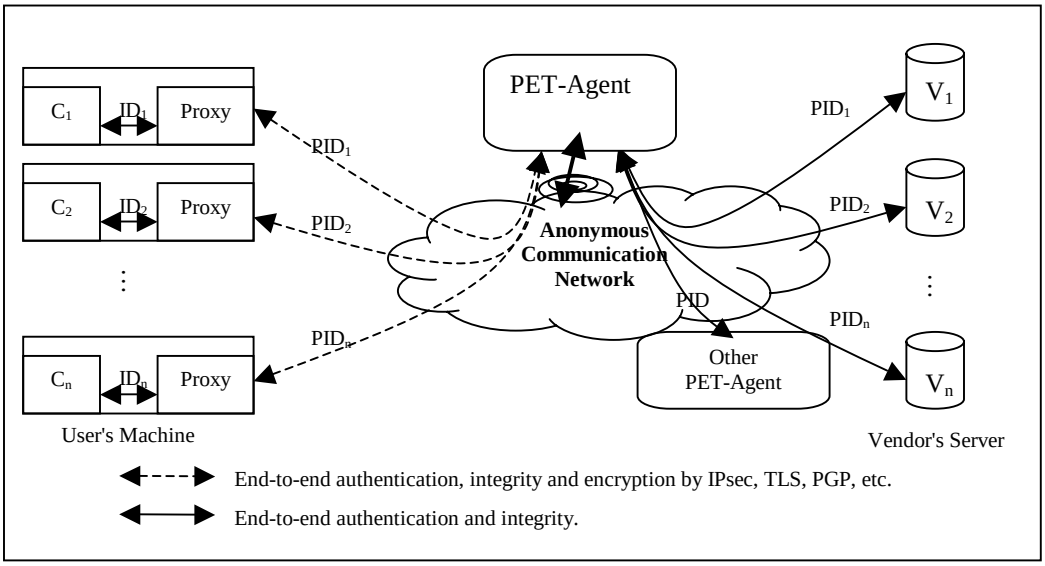


Figure 11. AII Model II over an anonymous network.

- ***Over anonymous communication network:*** Like the last configuration in the AII Model I, if the user uses a client-side identity protector proxy, the end-to-end security between the user and the PET-Agent and between the PET-Agent and the vender is still required. These security mechanisms can be provided with IPsec, TLS, openPGP, etc. Figure 11 depicts this configuration. This configuration can provide stronger anonymous protection against traffic analysis.

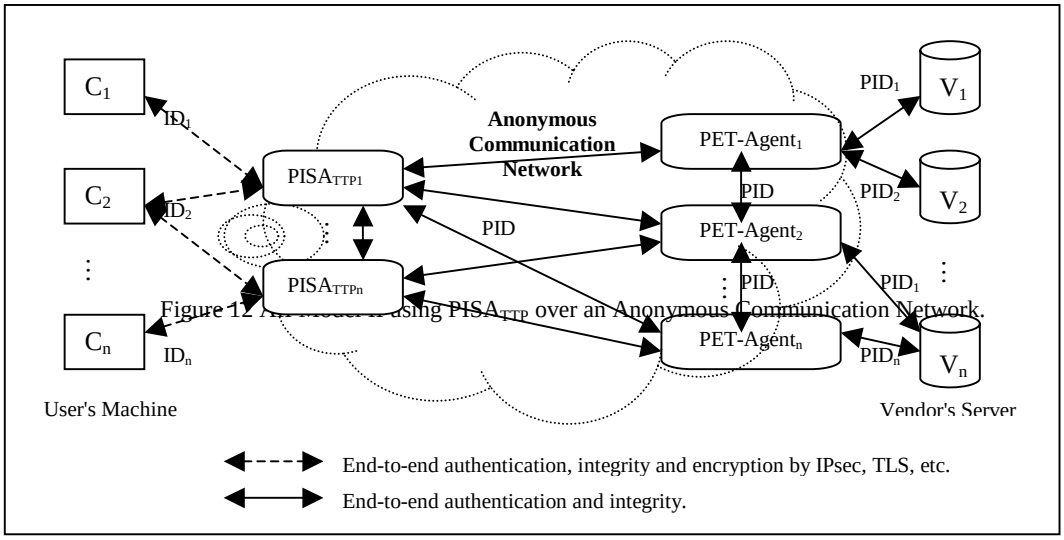


Figure 12. AII Model II using $PISA_{TTP}$ over an Anonymous Communication Network.

Figure 12. AII Model II over an anonymous network with $PISA_{TTP}$.

Another configuration in this model is for the user to use the $PISA_{TTP}$ as the identity protector. An end-to-end security between the user and the $PISA_{TTP}$, between the $PISA_{TTP}$ and the PET-Agent, between the PET-Agent and the venders is required. They can be provided with IPsec, TLS, openPGP, etc. Figure 12 depicts this configuration. This is our preferred model. It offers a stronger protection against threats to personal privacy.

## 4. Security Interface for PET-Agent

In order to provide a secure connection between the PET-Agent and the user's machine and between the PET-Agent and the vendor's server, some security protocol interfaces are necessary in the PET-Agent. In addition, some security APIs also are necessary for cryptographic services (e.g. RSA, DES, etc.), digital signatures (e.g. RSA, DSS, PGP, etc.), key management (e.g. ISAKMP, Kerberos, etc), certificate management (e.g. PKI, SPKI, etc), etc.

Based on the configuration models in our AII Model, we discuss these security interfaces in three different configurations, i.e. the PET-Agent over the normal Internet, a large intranet and an anonymous communication network, respectively.

### 4.1 PET-Agent over the normal Internet

In this situation, the PET-Agent should provide registration and security communication services including authentication, encryption and integrity services between the PET-Agent and the user. Since the PET-Agent over Internet, the available security protocols include IPsec, IKE, TLS, openPGP, S/MIME.

On the other hand, the PET-Agent should provide security communication services between the PET-Agent and the vendor's server. The available security protocols include IPSEC, IKE, TLS, openPGP, S/MIME.

### 4.2 PET-Agent over a large intranet

In this situation, since the user may access the PET-Agent using different techniques, the PET-Agent may need more security protocol interfaces. If the user is using remote access (e.g. dial-up, wireless, etc.), the PET-Agent should provide security protocol interfaces for RADIUS, AAA, etc. If the user is a local access user, the PET-Agent should provide security protocol interfaces for IPsec, TLS, openPGP, S/MIME.

Irrespective, like the PET-Agent over Internet, the PET-Agent should provide security protocol interfaces for IPsec, TLS, openPGP, S/MIME, VPN.

### 4.3 PET-Agent over an anonymous communication network

Since some anonymous communication networks cannot provide security services for VPN, IPSEC, etc., the available security protocols are fewer, e.g. TLS, openPGP, etc. This indicates that some new security protocols may need to be proposed, in order to solve these problems. Indeed, some new anonymous communication networks may support more security protocols (e.g. IPsec, ) in the future.

## 5. Pseudonym E-Commerce Model Based on PISA

Although the above AII Model provides anonymous protection for many application environments, such as the labour market, it is not enough to provide anonymous protection for some environments requiring payment function. In order to build a pseudonym e-commerce model with payment function, we need to introduce some new conceptions: Pseudonym E-bank, Pseudonym E-account, Pseudonym E-check.

- ***Pseudonym E-Bank:*** Pseudonym E-bank is an electronic bank that can issue some pseudonyms, private credentials and public key certificates for its customers, where public key certificate does not use the user's real identity, but use the user's pseudonym.
- ***Pseudonym E-Account:*** Pseudonym E-account is a pseudonym user's account that is registered by the user using his/her pseudonym and corresponding pseudonym public key certificate.
- ***Pseudonym E-Check:*** Pseudonym E-check is one kind of electronic check that has similar data format to the regular check, but uses digital watermark techniques for protection against forgery. In addition, the pseudonym e-check is valid only if it is signed using the right public key certificate that is registered in the user's pseudonym e-account. An on-line verification is required for payment.

Our pseudonym e-commerce model, based on PISA, consists of four entities: customer, vendor, PISA and pseudonym e-bank.

The communications among these entities consists of four protocols: pseudonym e-account registration protocol, customer-PISA interaction protocol, PISA-vendor interaction protocol and pseudonym payment protocol (e.g. SET). Figure 13 depicts pseudonym e-commerce model based on PISA. We assume all communication among the entities is over the insecure Internet. The security is provided by these security protocols.

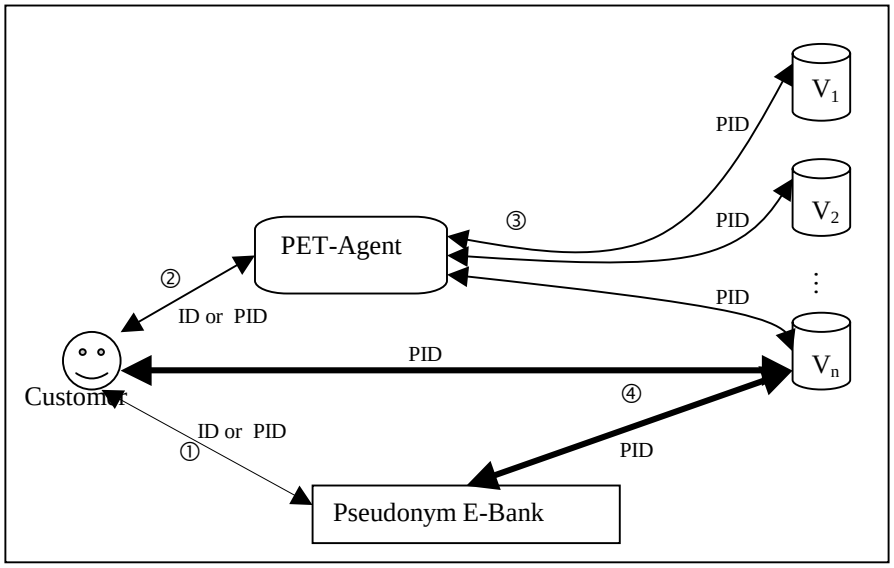


Figure 13. Pseudonym e-commerce model base on PISA

① ***Pseudonym E-account Registration Protocol:*** This protocol is used for opening a pseudonym e-account to its customers. A customer's account must be linked to his/her pseudonym public key certificate. Some protocols [4, 29] in the pseudonym systems can be used for this function.

② ***Customer-PISA Interaction Protocol:*** This protocol is used for interactions between the customers and PISA. Some protocols such as IPsec and TLS can be used for this function.

③ ***PISA-Vendor Interaction Protocol:*** This protocol is used for PISA seeking products' information from venders. Some protocols such as IPsec and TLS can be used for this function.

④ ***Pseudonym Payment Protocol:*** This protocol is used for anonymous payment among the customer, vendor and e-bank. SET protocol can be used for this function, but payment mechanism need to be modified to use on-line pseudonym e-check. The e-bank can protect the e-check's validity against copy by the check number, digital signature and valid date.

## 6. Conclusion

This document reviews the existing privacy protection techniques: pseudonym systems, PET and anonymous communication networks. We propose a model for an Anonymous Internet Infrastructure (AII), an anonymous Internet based on these techniques**.** This model focuses on some of the privacy requirements from the network perspective for Privacy Enhancing Technologies. It does not take into account several the non-network related issues associated with the PET. These include:

- Protection of data within a software agent.
- Protection of the code of a software agent from hostile hosts or agents.
- Specific approaches for anonymous or pseudonymous identity management.
- The application to meet privacy objectives of technologies developed for other areas. For instance, one of these include technologies is Intellectual Property protection or Digital Rights Management (DRM). These approaches offer a way of managing how and to whom intellectual property is distributed. DRM may be used to manage and track how private data is distributed.
- Secure distributed logs and other systems to provide privacy audit information for transaction traceability and accountability from a privacy point-of-view.

In addition, we will do further research on the pseudonym IP, an anonymous communication network at IP layer that can support any TCP/IP application. It will be a good choice for AII.

## Acknowledgments

We would like to thank all members of IIT at the NRC of Canada for their support towards our R&D project on Network Privacy Protection. We also thank our European Community partners in the Privacy Incorporated Software Agent (PISA), EU Fifth Framework Project.

## References

[1] A.back, I.Goldberg and A.Shostack. Freedom 2.1 Security Issues and Analysis. May 2001. Available at http://www.freedom.net/info/whitepapers/Freedom_Security2-1.pdf.

[2] A.Back. Hashcash. Available at http://www.cypherspace.org/~adam/hashcash/. March 1997.

[3] A.Juels and J.Brainard. Client Puzzles: A Cryptographic Defence against Connection Depletion Attacks. In S.Kent, editor, NDSS '99 (Networks and Distributed Security Systems), pages 151-165, 2000.

[4] A.Lysyanskaya, R.Rivest and A.Sahai. Pseudonym Systems. Selected Areas in Cryptography : 6th Annual International Workshop, SAC'99, Volume 1758 of Lecture Notes in Computer Science, pages 184-200, Springer-Verlag, 1999.

[5] The Anonymizer. Available at http://www.anonymizer.com.

[6] A.Pfitzmann, B.Pfitzmann and M.Waidner. ISDN-MIXes - Untraceable Communication with Very Small Bandwidth Overhead. Proc.Kommunikation in verteilten Systemen, IFB 267, pages 451-463, Springer-Verlag, 1991.

[7] A.Pfitzmann and M.Waidner. Network without User Observability. Computers & Security, vol.2, no.6, pages 158-166, 1987.

[8] A.Pfitzmann and M.Waidner. Networks without User Observability - Design Options. In Advances in Cryptology - Eurocrypt '85, Volume 219 of Lecture Notes in Computer Science, Springer-Verlag, 1985.

[9] C.Dwork and M.Naor. Pricing via Processing or Combating Junk Mail. In Ernest F.Brickell, editor, Advances in Cryptology - CRYPTO '92, Volume 740 of Lecture Notes in Computer Science, pages 139-147, Springer-Verlag, 1992.

[10] D.Chaum. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology, vol.1, no.1, pages 65-75, 1988.

[11] D.Chaum and J.Evertse. A secure and privacy-protecting protocol for transmitting personal information between organizations. In Advances in Cryptology—CRYPTO ’86, pages 118-167, Springer-Verlag, 1986.

[12] D.Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communication of the ACM, vol.28, no.10, pages 1030-1044, October 1985.

[13] D.Chaum. Blind signatures for untraceable payments. In R.L.Rivest, A.Sherman, and D.Chaum, editors, Proc.CRYPTO '82, pages 199-203, New York, 1983.

[14] D.Chaum. Untraceable Electronic Mail, Return Address, and Digital Pseudonyms. Communications of the ACM, vol.24 no.2, pages 84-88, 1981.

[15] Daemon9. Project neptune. Phrack Magazine, 48(7): File 13 of 18, 8 November 1996. Available at http://www.fc.net/phrack/files/p48/p48-13.html.

[16] D.Goldschlag, M.Reed and P.Syverson. Onion Routing for Anonymous and Private Internet Connections. Communication of the ACM, vol.42, no.2, pages 39-41, 1999.

[17] D.Goldschlag, M.Reed and P.Syverson. Hiding Routing Information. In R.Anderson, editor, Information Hiding: First International Workshop, Volume 1174 of Lecture Notes in Computer Science, pages 137-150, Springer-Verlag, 1996.

[18] D.Kesdogan, J.Egner and R.Buschkes. Stop-and-go MIXes Providing Probabilistic Security in an Open System. In David Aucsmith, editor, Information Hiding: Second International Workshop, Volume 1525 of Lecture Notes in Computer Science, pages 83-98, Springer-Verlag, 1998.

[19] D.R.Simon. Anonymous Communication and Anonymous Cash. In Advances in Cryptology – CRYPTO ’96, Volume 1109 of Lecture Notes in Computer Science, pages 61-73, Springer-Verlag, 1996.

[20] Private Credentials. Zero-Knowledge Systems, Inc. white paper, 2000. Available at http://www.freedom.net/info/whitepapers/credsnew.pdf.

[21] R.Samuels and E.Hawco. Untraceable Nym Creation on the Freedom 2.0 Network. Zero-Knowledge Systems, Inc. white paper, 2000. Available at http://www.freedom.net/info/whitepapers/Freedom-NymCreation.pdf.

[22] G.J.Simmons. The history of subliminal channels. IEEE Journal on Selected Area in Communications, vol. 16, no.4, pages 452-462, May 1998.

[23] I.Goldberg and A.Shostack. Freedom Network Whitepapers.

[24] I.Goldberg, D.Wagner and E.Brewer. Privacy-Enhancing Technologies for the Internet. In *Proceedings of IEEE COMPCON ’97*, pages 103-109, 1997.

[25] J.Bos. Detection of Disrupters in the DC Protocol. In Advances in Cryptology - Eurocrypt '89, Volume 434 of Lecture Notes in Computer Science, pages 320-327, Springer-Verlag, 1989.

[26] J.Borking. Proposal for Building a Privacy Guardian for the Electronic Age. In H.Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 130-140, Springer-Verlag, 2000.

[27] John Kelsey. Private Communication, 1999.

[28] J.Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In H.Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 10-29, Springer-Verlag, 2000.

[29] L.Chen. Access with pseudonyms. In Ed Dawson and Jovan Golic, editors, Cryptography: Policy and Algorithms, Volume 1029 of Lecture Notes in Computer Science, pages 232-243, Springer-Verlag, 1995.

[30] L.Cottrell. Mixmaster. Available at http://www.obscura.com/~loki/.

[31] L.Lamport, R.Shostak and M.Pease. The Byzantine Generals Problem. ACM TOPLAS, vol.4, no.3, pages 382-401, 1982.

[32] M.Pease, R.Shostak and L.Lamport. Reaching Agreement in the Presence of Faults. JACM, vol.27, no.2, pages 228-234, 1980.

[33] M.Reed, P.Syverson and D.Goldschlag. Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications, vol.16, no.4, pages 482-494, May 1998.

[34] M.Reiter and A.Rubin. Anonymous Web Transactions with Crowds. Communications of the ACM, vol.42, no.2, pages 32-48, 1999.

[35] M.Reiter and A.Rubin. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, vol.1, pages 66-92, 1998.

[36] M.Waidner. Unconditional Sender and Recipient Untraceability in Spite of Active Attacks. In Advances in Cryptology - Eurocrypt '89, Volume 434 of Lecture Notes in Computer Science, pages 302-319, Springer-Verlag, 1989.

[37] Mature NymIP Network: IP-Layer Desiderata. V1.1, October 2000. Available at http://nymip.velvet.com/cvs/general/zks-desiderata.html.

[38] O.Berthold, H.Federrath and S.Kopsell. Web MIXes: A System for Anonymous and Unobservable Internet Access. In H.Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 115-129, Springer-Verlag, 2000.

[39] P.Boucher, A.Shostack and I.Goldberg. Freedom Systems 2.0 Archtecture. December 2000. Available at http://www.freedom.net/info/whitepapers/Freedom_System_2_Architecture.pdf.

[40] P.Syverson, M.Reed and D.Goldschlag. Onion Routing Access Configurations. In DISCEX 2000: Proceedings of the DARPA Information Survivability Conference and Exposition, Hilton Head, SC, IEEE CS Press, pages 34-40, January 2000.

[41] R.Hes and J.Borking. Privacy-Enhancing Technologies: The Path to Anonymity. Revised Edition. A&V-11. Den Haag: Registratiekamer, 1998.

[42] S.A.Brands. Restrictive blinding of secret-key certificates. Technical Report CS-R9509, CWI-Certrum voor Wiskunde en Informatica, February 28, 1995.

[43] S.Dolev and R.Ostrovsty. Efficient Anonymous Multicast and Reception. In Walter Fumy, editor, Advances in Cryptology - EUROCRYPT '97, Volume 1233 of Lecture Notes in Computer Science, pages 395-409, Springer-Verlag, 1997.

[44] W.Dai. Pipenet 1.1. Available at http://www.eskimo.com/~weidai/pipenet.txt, 2000.

[45] W.Dai. Private Communication, 1999.

[46] N.Zhang, Q.Shi and M.Merabti. Anonymous Public-key Certificates for Anonymous and Fair Document Exchange. IEE Proceedings Communication, vol.147, no.6, pages 345-350, December 2000.

[47] K.Oishi, M.Mambo and E.Okamoto. Anonymous Public Key Certificates and Their Applications. IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E81-A, (1), pages 56-64, 1998.

[48] F.Bao, R.Deng and W.Mao. An efficient and Practical Fair Exchange Protocols with Off-line TTP. Proceedings of IEEE symposium on security and privacy, Oakland, California, USA, pages 77-85, May 1998.

[49] D.Davies, D.Barber, W.Price and C.Solomides. Computer Networks and their Protocols. John Wiley and Sons, 1979.

[50] O.Berthold, H.Federrath and M.Kohntopp. Project "Anonymity and Unobservability in Internet". Available at http://www.inf.tu-dresden.de/~hf2/publ/2000/BeFK2000cfp2000/.

[51] I.Goldberg. A Pseudonymous Communications Infrastructure for the Internet. Ph.D. thesis, University of California at Berkeley, Fall 2000.

## Biography

**Ronggong Song** received his B.Sc degree in mathematics in 1992, M.Eng degree in computer science in 1996, Ph.D. in network security from Beijing University of Posts and Telecommunications in 1999. He had employed as Network Planning Engineer at Telecommunication Planning Research Institute of MII, P.R.China, and Postdoctoral Fellow at University of Ottawa, Canada. Now, he is working at NRC of Canada. His research interests are privacy protection, network security, e-commerce, IP mobility and QoS.

**Larry Korba** is the group leader of the Network Computing Group of the National Research Council of Canada in the Institute for Information Technology. He is the leader of the Canadian contribution to the Privacy Incorporated Software Agent (PISA) project. His research interests include privacy protection, network security, and computer supported collaborative work.