Ensuring Privacy for Buyer-Seller E-Commerce[1]

George Yee, Larry Korba, and Ronggong Song

Institute for Information Technology
National Research Council Canada
1200 Montreal Road, Building M-50, Ottawa, ON, Canada K1A 0R6
{George.Yee, Larry.Korba, Ronggong.Song}@nrc-cnrc.gc.ca
http://www.iit-iti.nrc-cnrc.gc.ca

Abstract. The growth of the Internet has been accompanied by the growth of e-services (e.g. e-commerce, e-health). This proliferation of e-services and the increasing regulatory and legal requirements for personal privacy have fueled the need to protect the personal privacy of e-service users. Existing approaches for privacy protection such as the use of pseudonym technology, and personal privacy policies along with appropriate compliance mechanisms are predicated on the e-service provider having possession and control over the user's personal data. In this paper, we propose a new approach for protecting personal privacy in buyer-seller e-commerce: keeping possession and control over the buyer's personally identifiable information in the hands of the buyer as much as possible, with the help of a smart card and a trusted authority. Our approach can also be characterized as distributing personally identifiable information only on a "need to know" basis.

1 Introduction

This work presents a new approach for protecting personal privacy in buyer-seller e-commerce. The approach is based on keeping possession and control over the buyer's personally identifiable information in the hands of the buyer as much as possible.

The motivation for this approach comes from the fact that once buyer personal information is in the hands of a seller, it becomes very difficult to ensure that the seller will respect the buyer's privacy preferences. In addition, it is a hard problem to guarantee that a seller will not circumvent any kind of private data access control that might be in place. We were therefore led to the following proposition: let the buyer, as much as possible, not transfer his/her personally identifiable data to the seller but instead keep it in his/her possession and retain control over it.

Our proposed approach employs selective disclosure of the buyer's information and a smart card, in conjunction with the buyer's personal privacy policy, to keep *control* of the buyer's personally identifiable data in the hands of the buyer as much as possible, rather than in the hands of the seller.

We use the term "bse-service" to mean "buyer-seller e-service", a service that consists of the purchase of goods by a buyer from a seller across the Internet (e.g.

[1] NRC Paper Number: NRC 48461

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

Amazon.com). Goods may be physical (e.g. computers) or informational (e.g. stock quotes). The service is performed by application software (service processes) that is owned by the seller. The seller has a privacy policy that spells out what buyer personal information is needed for its service and how the personal information will be handled. The buyer has a personal privacy policy that defines what personal information he/she is willing to disclose and how that information is to be handled by the seller.

In the literature, elemental components of our proposal exist, but not, as far as we can tell, assembled into the approach presented here. For example, Clarke [7] wrote about smart cards (he actually was complaining that their use destroys privacy), anonymity, and the use of pseudonyms and trusted third parties. Laudon [8] suggested that individuals could sell their private information in an information market, and thus maintain control over their private information (the maintaining control part is similar to what we propose here but the means for doing so is completely different). However, Laudon's proposal is flawed in that it does not discuss the potential abuse of private information in a market setting (e.g. theft).

Smart cards have been around for over 3 decades and have been applied across many domains including e-commerce [1, 2]. Their computational, memory, and security features make them ideal for portable data applications requiring security [2].

Figure 1 (adapted from [9]) gives an example of buyer/seller privacy policies for an online pharmacy. *Policy Use* indicates the type of online service for which the policy will be used. *Valid* holds the time period during which the policy is valid. The required fields (e.g. collector, what) of these policies are derived from Canadian privacy legislation [9]. This legislation is a good source for deriving privacy policies since it is representative of privacy legislation in many countries. These are minimum privacy policies in the sense that the fields *collector*, *what*, *purposes*, *retention time*, and *disclose-to* form the minimum set of fields required to satisfy the legislation for any one information item. Each set of such fields is termed a *privacy rule* describing a particular information item. Privacy policies need to be machine-readable and may be expressed using a XML-based language such as APPEL [3].

Policy Use: *Pharmacy* Owner: *Alice Buyer* Valid: *unlimited*	Privacy Use: *Pharmacy* Owner: *A-Z Drugs Inc.* Valid: *unlimited*
Collector: A-Z Drugs Inc. *What:* name, address, tel *Purposes:* identification *Retention Time:* unlimited *Disclose-To*: none	*Collector:* Drugs Dept. *What:* name, address, tel *Purposes:* identification *Retention Time:* 1 year *Disclose-To*: none
Collector: A-Z Drugs Inc. *What:* drug name *Purposes:* purchase *Retention Time:* 2 years *Disclose-To*: none	*Collector:* Drugs Dept. *What:* drug name *Purposes:* sale *Retention Time:* 1 year *Disclose-To*: none

Fig. 1. Example buyer (left) and seller (right) privacy policies.

Note that all information that the buyer discloses to a seller is considered personal information and described in the buyer's personal privacy policy. Some of this information is personally identifiable information (PII), i.e. the information can identify the buyer. For example, "name", "address", and "telephone number" are PII. There may be other information described in a personal privacy policy that is not personally identifiable information (non-PII), i.e. the information by itself cannot identify the buyer. For example, the selection of Aspirin as a medication at an online pharmacy cannot normally identify the buyer.

Section 2 presents our approach for using selective disclosure and smart cards to protect consumer personal information. Section 2 also gives an example of applying our approach. Section 3 presents our conclusions and plans for future research.

2 Using Selective Disclosure and Smart Cards to Protect Privacy

Our goal is to protect a buyer's privacy according to his/her personal privacy policy. This policy can be violated by the seller (or other potential attackers) who would normally be in possession and control of the buyer's submitted personal information. Our answer to privacy protection is simple: *remove the buyer's PII from the possession and control of the seller.* We accomplish this by having the buyer's personal information in a smart card, called a *privacy controller*, owned by the buyer and in his/her possession. The personal information in the privacy controller can only be entered and accessed by the buyer. Using the privacy controller, the buyer is able to selectively disclose (explained below) his/her PII only when necessary, not to the primary service provider (i.e. the seller), but to trusted support providers that support the primary provider with business services that do require the user's PII. Further, the privacy controller smart card will process the buyer's PII according to his/her privacy policy. The buyer is anonymous to the seller at all times.

We require that the primary service can do without the buyer's PII. For this to be true, the primary service must be decomposable into components that do and do not need the user's PII. For example, bse-services can be decomposed into three components, namely order entry and processing, order delivery, and order payment, in which only order delivery and order payment may need the user's PII. In fact, for informational services, the network delivery of information may even do without the user's PII (i.e. allow him/her to be anonymous), through the use of anonymous communications (e.g. using a MIX network such as JAP [10]). Thus, the primary service provider or seller does not need the buyer's PII but makes use of support services that do need the PII, namely shipping (for physical goods) and payment services from other providers. Paypal [6] is an example of a payment service provider.

We further require the services of a trusted authority (a Certificate Authority with an extended role) to program the smart card to act as a privacy controller, to keep the true identity of the user should there be a need to recover it (e.g. in legal proceedings), and to distribute the smart card. Figure 2 illustrates our approach.

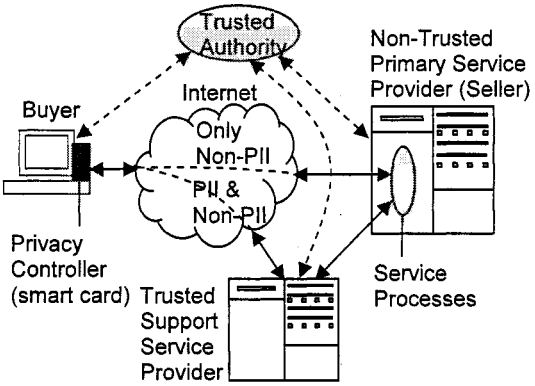

Fig. 2. Using selective disclosure and smart card to protect buyer privacy.

Our approach is really applying the need-to-know principle to bse-services, distributing PII only where appropriate. A bse-service is decomposed into a *primary service* that does not require PII and *support services* that do require PII but are trusted to maintain the anonymity of the buyer. The user's privacy controller discloses PII only to the support services that require the buyer's PII.

2.1 Selective Disclosure and Resultant Privacy Policy Transformations

The redirection of PII from the primary service provider to support service providers necessitates the controller updating the privacy rules in the buyer's policy. Thus, if the online pharmacy for Figure 1 uses a trusted shipper, Global Shipping Inc., the first rule in the consumer policy (see Figure 1) would be transformed to:

Collector: Global Shipping Inc.
What: name, address, tel
Purposes: shipping
Retention Time: unlimited
Disclose-To: none

The controller knows the destination of the re-direction from information provided by the primary service provider. The corresponding rules in the privacy policy of the primary service provider would already reflect such destinations, since it is set up to make use of support providers. In this way, the buyer has only to deal with the primary service provider in his/her privacy policy.

2.2 Privacy Controller and Service Process Requirements

The privacy controller processes each privacy rule component in the buyer's privacy policy as follows:

a) *Collector*: Confirm that the collector named by the service processes is the collector specified in the buyer's policy.
b) *What*: Confirm that the information item requested by the service processes is as specified in the buyer's policy.
c) *Purposes*: Confirm that the purposes for which the information will be used are as specified in the buyer's policy.
d) *Retention Time*: Destroy the buyer's personal information at the end of its retention time.
e) *Disclose-To*: Confirm that the receiving party in the case of a disclosure request is the party specified in the buyer's privacy policy.

The service processes must cooperate with the privacy controller where necessary in order to carry out the above requirements (e.g. provide the seller's privacy policy to the privacy controller).

These requirements dictate the functionality of the privacy controller and the primary service processes (PSP). The privacy controller, in acting to ensure compliance with the buyer's privacy policy, runs in two phases as described below. In phase 1, the controller essentially transforms the buyer's policy for PII redirections and compares policies. In phase 2, the controller enforces the buyer's privacy policy. Phase 2 can only be reached if phase 1 is successful (if phase 1 is unsuccessful, the buyer and seller can enter into negotiation [5] failing which the buyer can choose another seller).

Privacy Controller Processing for Buyer Privacy Policy Compliance. In phase 1 (see Figure 3),

- Establish a connection to the seller and download the seller's privacy policy and support service provider information.
- Transform the buyer's privacy policy for PII redirections, as described above.
- Verify that the privacy rules in the seller's privacy policy matches the privacy rules in the buyer's privacy policy (comparing privacy policies for a match is outside the scope of this paper but see [4]). If this verification fails, inform the buyer and terminate (or negotiate privacy policies as indicated above). Otherwise, proceed to phase 2.

In phase 2,

- Prompt buyer for each information item (II) and accept only II of the types specified in the buyer's privacy policy.
- Store buyer's II in its personal information store.
- Destroy the buyer's II if the retention time is up.
- Disclose only non-PII to the PSP as described above.
- Accept requests from the PSP to disclose the buyer's II (PII and non-PII) to support service providers as allowed by the buyer's privacy policy, passing along the II's retention time. These support providers are not allowed to further disclose the buyer's PII. Note: the typical buyer would normally not be receiving disclosures. In this work, only providers receive disclosures, e.g. a trusted shipping company receiving an address disclosure for shipping purposes.

Service Processing. The PSP executes during the controller's phase 2 processing, as follows:

- Perform normal processing for the service that is offered by the seller, including requesting non-PII from the privacy controller needed for service processing.
- If needed, request the controller to disclose information to trusted support providers.

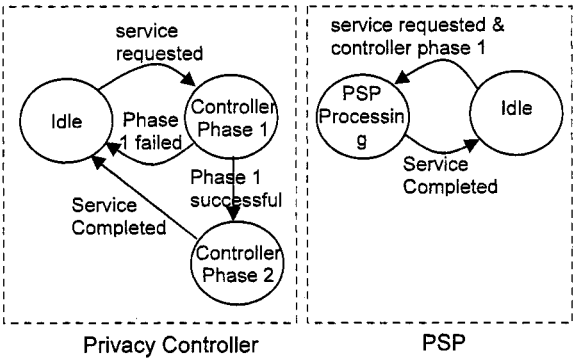

Fig. 3. High-level state machines for privacy controller and PSP.

2.3 Role of the Trusted Authority and Additional Operational Details

The trusted authority is a certificate authority with an extended role, called an extended CA or "eCA" for short. Prior to the commencement of any bse-service, the eCA works to familiarize sellers and buyers with its services. Sellers can "subscribe" to the eCA and arrange their service processes to work with the privacy controller smart card (e.g. conform to smart card interfacing requirements). The smart card is remotely programmed by the eCA to be used as the privacy controller and to work with the sellers that have subscribed to the eCA (e.g. download seller's privacy policy, upload buyer's information). The programming automatically allows the smart card to be used with new sellers that may subscribe to the eCA later. The eCA distributes these smart cards to service users through local electronics outlets (e.g. Best Buy). When purchased at a local electronics outlet, the smart card only has the ability to automatically connect to the eCA (in addition to normal smart card functions). The eCA also selects and confirms a number of support providers as trusted parties for business services such as shipping and payment. Further, the eCA issues digital certificates to all sellers for use in authenticating themselves.

A buyer who wants to buy from sellers that subscribe to the eCA registers with the eCA's web site through a secure channel. After paying the eCA an appropriate fee using a secure credit card transaction, the buyer receives from the eCA a number of different pseudonyms and a digital certificate (for authentication purposes) that identifies the buyer using the pseudonyms (one pseudonym for each seller the buyer wants to use). In processing the buyer's credit card, the eCA also checks the buyer's name, address information, and credit history with the credit card company.

To use a bse-service, the buyer connects the smart card to a USB port on his/her computer. The buyer is automatically connected to the eCA's website after mutual authentication (using digital certificates) through a secure channel. The eCA then

remotely programs the smart card for use as a privacy controller, instructing the controller to use the buyer's pseudonyms for identification purposes with bse-service providers (one pseudonym with each provider) (note: this is done only if the smart card has not been programmed previously). The buyer is then allowed to select which seller to use. After the buyer selects the seller, the website prompts the buyer to enter a privacy policy to be used with the selected seller if this is the buyer's first use of the seller. Note that the website is better equipped with appropriate graphical interfaces than the smart card for the buyer to enter a privacy policy. The entered policy or a previously entered policy (they are stored on the eCA's website) is then automatically downloaded to the smart card. At this point, the controller automatically begins phase 1 processing. A pop-up window appears indicating an anonymous connection to the bse-service with successful 2-way authentication through a secure channel and with the seller's privacy policy downloaded (controller phase 1 processing). The privacy controller then transforms the buyer's policy for PII redirections and compares the buyer's privacy policy (previously entered) with the provider's privacy policy for compatibility. If this is successful, the privacy controller initiates phase 2 processing. Otherwise, the privacy controller initiates a privacy policy negotiation session with the seller that takes place via the privacy controller. If this negotiation is successful, the privacy controller can begin phase 2. If neither the original phase 1 nor the negotiation is successful, the buy must choose a different seller. Once the controller starts phase 2, the seller's service processes are initiated. The latter then requests non-PII from the controller and requests it to send information disclosures (possibly sending PII to trusted parties (e.g. address for shipping)) as the service requires. Service output is sent back to the user via the controller-service processes channel.

It follows from the above that the eCA can link the user's pseudonym with the user. This is allowed on purpose, so that when necessary the seller can request the true identity of the buyer. For example, this may be necessary in a medical emergency where an e-pharmacy seller needs to contact the buyer, or where there is a dispute involving the buyer, and the buyer's real name is needed for legal proceedings.

2.4 Security Measures

Based on the above operating scenarios, the vulnerability areas include: a) storage of personal data, b) distribution of the smart card through local electronic outlets, c) sending data disclosures, d) communication between the privacy controller and the service processes, and between the buyer and the eCA's web site, e) disclosure of non-PII to the service processes, i.e. although the data is non-PII, could their combinations collected over time compromise the anonymity of the buyer? f) traceable communications over the Internet, g) dishonest parties masquerading as trusted parties, h) Trojan horse programs in the buyer's computer, and i) the buyer loses his/her smart card, either by accident or theft.

We discuss our security measures for each vulnerability area in turn as follows:

a) Storage of personal data: the data is secured on the smart card (processor-enabled) using symmetric encryption (e.g. 3DES). The key for the encryption algorithm can be generated (e.g. using a SHA-2 hash function) by the smart card from the user's password for accessing the card. Further, the smart card incorporates a locking mechanism that locks out any attacker who tries to access

the card by trying to guess the password – the locking mechanism can lock the user out, for example, after 5 tries. Thus, the attacker first of all cannot access the card because he/she does not know the password. Even if the attacker uses some special technology to get at the data, he/she cannot read it since it is encrypted. Finally, the attacker cannot decrypt the data because he/she again does not know the password, used to generate the encryption key. To protect the password from Trojan horses, the password mechanism and storage is physically isolated from the area of the smart card that can connect to the Internet.

b) Distribution of the smart card through local electronic outlets: the risk is that an attacker could modify the card before it is sold to i) connect to a fake website controlled by the attacker, or ii) introduce malware into the card that would later play havoc with any programming; possibility i) is defeated by required mutual authentication between the user and the eCA; possibility ii) can be defeated using built-in card self sanity checks together with malware detection software run on the card by the eCA prior to remote programming.

c) Sending / receiving data disclosures: the privacy controller establishes a secure channel (SSL or secure VPN) to the receiving party for use in data conveyance; the sending controller authenticates the receiving party using the receiving party's digital certificate before any data is sent. Receiving parties are pre-screened by the eCA, who issues them digital certificates for authentication purposes.

d) Communication between privacy controller and service processes: the controller establishes a secure channel (SSL or secure VPN) to the service processes to be used for communication purposes. The controller authenticates the service processes using their digital certificates issued to them by the eCA. Similarly, the service processes authenticates the controller using the digital certificate issued to the buyer by the eCA. This same secure procedure is used for communication between the user and the eCA's website.

e) Disclosure of non-PII leads to compromising anonymity: we believe that this risk is minimal for bse-services. Identity discovery from non-PII depends on the size of the buyer population, the method of selective disclosure, and the amount of non-PII data in circulation pertaining to the individual. This risk can be minimized if the buyer population is the whole Internet community. However, some bse-services operate only regionally so this may not apply. Next, this risk may be further minimized by employing more effective methods for selective disclosure. Finally, bse-services require minimal non-PII, resulting in minimal non-PII data in circulation for any one individual, thereby further reducing this risk.

f) Traceable communications over the Internet: the controller not only establishes a secure channel for communication with the service processes but establishes it using a MIX network (e.g. JAP [10]). By so doing, the seller would find it very difficult to trace the identity of the buyer using the buyer's Internet connection.

g) Dishonest parties masquerading as trusted parties: first, the reputation of the eCA is established (as for a regular CA); for example, the eCA could be subjected to inspection audits and other forms of testing to ensure that processes and responsibilities carried out are trustworthy. After the eCA is established to be trustworthy, it has the responsibility to make sure that all trusted support

providers are indeed trustworthy, perhaps by using a similar series of inspections and testing as was done for it.

h) Trojan horse programs running in the buyer's computer could modify the buyer's privacy policy or redirect the buyer's PII disclosures to the attacker. However, this data is only in transit to/from the smart card and would be encrypted. Further, the user can regularly run diagnosis software that identifies and deletes the offending programs.

i) If the buyer loses his/her smart card either by accident or theft, the person who finds the smart card or the person who stole it could masquerade as the original owner and incur services at that owner's expense or could somehow gain access to the original owner's PII. To reduce the risk of this happening, as mentioned in a), the smart card requires a password for access and has a locking mechanism that locks out the attacker after a fixed number of attempts (e.g. 5) to try and guess the password. If the legitimate buyer were to forget this password, the eCA could reset it through a secure connection to the eCA's website.

2.5 Security Vulnerability Analysis

We affirm the security of our approach by analyzing some possible attacks to see if they have any chance of success.

- *Substitution attack* – the attacker replaces the privacy controller with a version that appears to function normally but allow the covert capture of the user's PII. *Chance of success: very low – since the smart card requires a password and has a locking mechanism as described in Section 2.4(a).*
- *Modification attack* – the attacker modifies the privacy controller in order to obtain copies of the user's PII. This includes malicious attempts to read the PII from the store of the privacy controller. *Chance of success: very low – the data is encrypted and the key is produced from the card access password as the seed. Attempts at guessing the password are limited by the smartcard's locking mechanism.*
- *Man-in-the-middle attack* – the attacker makes copies of the user's PII disclosures on their way to the recipients (e.g. trusted shipping company). *Chance of success: low – the PII is sent using a secure channel. Similar answer (i.e. use of a secure channel) for such an attack on the communication between the buyer and the eCA's web site.*
- *Support provider spoofing attack* – the attacker pretends to be the legitimate recipient of a disclosure involving PII and captures the buyer's PII. *Chance of success: very low – the fake recipient would fail authentication by the sending controller.*
- *eCA spoofing attack, including web site phishing* – the attacker pretends to be the eCA and programs the buyer's smart card to steal the buyer's PII for the attacker. *Chance of success: very low – the fake eCA would fail authentication.*
- Privacy policy attack – the attacker modifies the user's and provider's privacy policies to possibly direct PII disclosures to self (if allowed by the PSP) or to extend the retention time hoping that more time will allow a modification attack to succeed. Chance of success: very low – the privacy policies are encrypted while on

route to the privacy controller. Further, both policies are securely stored at all their locations. See also Section 2.4(h).

- Inferred identity attack on the PSP – the attacker captures a user's non-PII by compromising the PSP; the attacker accumulates this data over a long period of time in the hope that by analyzing the data, some pattern will emerge that will identify the user. Chance of success: low – already discussed above in Section 2.4(e).
- Inferred identity attack on the SSP – the attacker captures a user's PII by compromising the SSP. Chance of success: low – depends on how well the SSP is protected from attack – since the provider is trusted, the eCA would have made sure that all appropriate safeguards were in place.
- Seller collusion attack to identify a buyer by linking pseudonyms – Chance of success: very low – a buyer's privacy controller automatically uses a different pseudonym with each seller.
- Support provider insider attack – the support provider becomes untrustworthy and compromises the user's anonymity. Chance of success: low – as mentioned in Section 2.4(g), the eCA has the responsibility to ensure that the support provider is trustworthy, not only at one time but all the time, perhaps by subjecting the support provider to regular and spontaneous inspection audits and testing.

The above brief analysis shows that our security measures are not fool proof against attacks, but probably provide enough of a deterrent to discourage most attacks.

2.6 Application Example

Consider an online pharmacy, E-Drugs, Inc. (fictitious name), that has subscribed to use the privacy protection services of Privacy Watch, Inc. (fictitious name), the eCA that has implemented our approach.

1. Alice, wishing to anonymously fill an electronic prescription, discovers by browsing PW's website that E-Drugs is available as a PW-subscribed seller.
2. (Omit this step if Alice has purchased from a PW seller before.) Alice registers with PW and is assigned a number of pseudonyms to be used as identification with sellers, e.g. a seller only knows Alice as "Patient21". She also receives a digital certificate from PW to be used for authentication purposes. Alice purchases a PW-issued smartcard from a local electronics outlet.
3. Alice connects her smart card to the USB port on her computer. After successful mutual authentication, she is connected to PW's web site via a secure channel.
4. (Omit this step if Alice has purchased from a PW seller before.) PW remotely programs Alice's smart card to be used as her privacy controller.
5. PW requests Alice to select a seller. After she selects E-Drugs, and enters her personal privacy policy on PW's web site (only if not previously entered for this seller), the privacy controller downloads Alice's privacy policy to the smart card. The controller is then connected to the service processes at E-Drugs automatically and anonymously through a secure channel and mix network. After successful mutual authentication, the controller downloads E-Drugs' privacy policy. After successfully transforming Alice's policy for PII redirections and

verifying that her privacy policy is compatible with E-Drugs' privacy policy, the privacy controller requests Alice's electronic prescription, shipping address, and credit card number.

6. Alice enters the requested information (disk location for the prescription) on her computer with the privacy controller making sure that the information corresponds with her privacy policy. The information is securely stored in the privacy controller. Upon request from E-Drugs' service processes, and after checking again with Alice's privacy policy, the controller discloses to the service processes details about the prescription (including the digital signature of the prescribing physician) but withholds Alice's name, address, and credit card number. Upon request from E-Drug's service processes, the controller sets up a secure channel to a trusted payment center (support provider) and authenticates the payment center before disclosing to the center Alice's credit card number. The trusted payment center maintains the patient's anonymity to the outside world by keeping the pseudonym-patient link secret (as do all trusted support providers). The trusted payment center was designated as trusted by PW beforehand and issued a digital certificate for authentication purposes. Similarly, the controller discloses Alice's name and address to a trusted shipping center that also keeps the pseudonym-patient link secret. Both the trusted payment center and the trusted shipping center use the pseudonym-patient link to link the order to the patient. If the patient tried a re-use attack to fill the prescription more than once, this would be detected by both these support providers through the pseudonym-patient link.
7. Alice receives her order the next day from the trusted shipping center.

3 Conclusions and Future Research

We have presented a novel approach to protect the privacy of buyers in buyer-seller e-commerce based on keeping control of the PII in the hands of the buyer, trusted support service providers, and an eCA acting as a trusted authority. In this approach, we chose to use a smart card for its portability, secure storage capability, and the fact that it needs to be connected to the Internet only for the duration of a service, reducing the risk of an Internet originated attack. Our approach may be characterized as distributing PII on a "need to know" basis and as a generalization of the use of trusted support providers such as Paypal [6] to protect privacy.

We believe our approach is very usable. The process of registering with the eCA is similar to the current way of registering with websites for a service or membership. The user only has to get the smart card once and can use it with all existing and new sellers that subscribe to the eCA. The user only has to plug the smart card in a USB port on his/her computer to begin the process of connecting to a service. Further, smart card use has been growing at a high rate, in part because the way they are used is similar to how millions of people use magstripe cards to access their bank accounts.

Some other advantages of our approach is that it is straightforward, employs existing technology, and would be fairly easy to set up. Another advantage is that the privacy controller automatically discloses private information according to the user's privacy policy. The extra costs of setup and operation for our approach could be

recovered from increased sales due to buyers feeling more comfortable that their privacy is protected.

A possible issue with our approach is that the use of a single eCA is a point of vulnerability and represents a monopoly situation. A possible resolution might be the use of several eCAs where each eCA has its provider or seller following. The buyer can then choose which eCA he/she would like to use based on the providers or sellers available at each respective eCA web site.

In terms of how security is weakened or strengthened, the use of an eCA is probably comparable to the use of a CA for PKI (Public Key Infrastructure).

As part of future research, we would like to address any issues with our approach and develop improved algorithms for selective disclosure to reduce the risk of patterns in disclosed non-PII that can identify the user.

References

1. Shelfer, K.M., Procaccino, J.D.: Smart Card Evolution. Communications of the ACM, Vol. 45, No. 7 (2002) 84
2. Carr, M.R.: Smart card technology with case studies. Proceedings, 36th Annual International Carnahan Conference on Security Technology (2002) 158-159
3. W3C: A P3P Preference Exchange Language 1.0 (APPEL 1.0). Accessed April 22, 2004 at: http://www.w3.org/TR/P3P-preferences/
4. Yee, G., Korba, L.: Comparing and Matching Privacy Policies Using Community Consensus. Proceedings, 16th IRMA International Conference, San Diego, California (2005)
5. Yee, G., Korba, L.: Bilateral E-services Negotiation Under Uncertainty. Proceedings, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida (2003)
6. Paypal. Accessed June 20, 2005 at: https://www.paypal.com/
7. Clarke, R.: Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue. Accessed October 3, 2005 at: http://www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html
8. Laudon, K.C.: Markets and Privacy. Communications of the ACM, Vol. 39, No. 9 (1996)
9. Yee, G., Korba, L.: Semi-Automatic Derivation and Use of Personal Privacy Policies in E-Business. International Journal of E-Business Research, Vol. 1, No. 1, 54-69. Idea Group Publishing (2005)
10. JAP. Accessed June 20, 2005 at: http://anon.inf.tu-dresden.de/desc/desc_anon_en.html

http://www.springer.com/978-0-387-33405-9

Security and Privacy in Dynamic Environments
Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May 2006, Karlstad, Sweden
Fischer-Hübner, S.; Rannenberg, K.; Yngström, L.; Lindskog, S. (Eds.)
2006, XVI, 494 p., Hardcover
ISBN: 978-0-387-33405-9