Pseudonym Technology for E-Service

Song, Ronggong; Korba, Larry; Yee, George

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Pseudonym Technology for E-Services *

Song, R., Korba, L., and Yee, G.
2006

* published in Privacy Protection for E-Services, published by Idea Group Inc. 2006. NRC 48269. Yee, G. (Editor)

Canada

Pseudonym Technology for E-Services[1]

Ronggong Song

National Research Council Canada, Canada

Larry Korba

National Research Council Canada, Canada

George Yee

National Research Council Canada, Canada

ABSTRACT

Pseudonym technology is attracting more and more attention and, together with privacy violations, is becoming a major issue in various e-services. Current e-service systems make personal data collection very easy and efficient through integration, interconnection, and data mining technologies since they use the user's real identity. Pseudonym technology with unlinkability,

anonymity, and accountability can give the user the ability to control the collection, retention, and distribution of his personal information. This chapter explores the challenges, issues, and solutions associated with pseudonym technology for privacy protection in e-services. To have a better understanding of how the pseudonym technology provides privacy protection in e-services, we describe a general pseudonym system architecture, discuss its relationships with other privacy technologies, and summarize its requirements. Based on the requirements, we review, analyze, and compare a number of existing pseudonym technologies. We then give an example of a pseudonym practice – e-wallet for e-services and discuss current issues.

KEYWORDS: pseudonym, pseudonym technology, anonymity, privacy, privacy protection, service, e-service, web service

INTRODUCTION

Background and Context

E-services such as e-commerce, e-government, e-health, and e-learning are becoming part of everyday life, and together with the Internet have come to be seen as an information infrastructure for every subject and many application domains. The tremendous growth of the varied e-services has catapulted them from their original realm of academic research towards new mainstream acceptance and increasing social relevance. However, this dramatic increase has

created the potential of eroding personal privacy. The fact is that cyberspace has invaded private space. Currently, almost all of the online e-services can be monitored by some unseen parties on the Internet. Controversies about cookies, click streams, traffic analysis, packet sniffing, and spam form merely the tip of an iceberg. It is small wonder that privacy is such a critical issue for e-services. Users feel that one of the most important barriers to using e-services 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.

According to the definition given by Goldberg in 1997 (Goldberg et al., 1997), privacy refers to the ability of individuals to control the collection, retention, and distribution of information about themselves. This doesn't mean that their personal information never gets revealed to any others. However, a system that respects their privacy should allow them to select what information about them is revealed, and to whom. This personal information may be any of a large number of items, including their shopping habits, nationality, work history, living habits, personal communications, email address, IP address, physical address, identity, and others.

Recently, many new techniques have been developed for providing privacy protection. Privacy protection is a process of finding an appropriate balance between privacy and multiple competing interests. Generally, they can be summarized into several kinds of techniques. One technique is the use of pseudonym technology for providing both anonymity and accountability. Another

is the use of an anonymous communication network for providing anonymity and unobservability. A third is the use of personal privacy policies along with secure mechanisms to guarantee that e-service providers conform to these policies (Yee & Korba, 2005).

A pseudonym is a fake name or alias, for instance, a user's digital account in a bank, an access account for a Web service. However, these pseudonyms are not protected with any special technologies so that they can be easily linked to the real identity of the user. We name the special technologies as pseudonym technologies which can prevent service providers from linking a pseudonym to the real identity of the user. With pseudonym technology, users can access the e-services by their pseudonyms instead of their real identities while still allowing the system to authenticate them as valid users. Furthermore, the system not only cannot link the pseudonyms with the real identities but also cannot link the pseudonyms used for different applications. This gives the users certain privacy protection and the service provider essential security protection. For instance, the users can protect their personal information and shopping habits if they use pseudonym-credentials (e.g. e-cash) to access some e-services or order some products. At the same time, the service providers or retail sellers can authenticate the credentials and users anonymously to reduce a variety of risks (e.g. fraud, repudiation) and protect their services. Pseudonym technology provides a good solution to privacy and security protection for most e-services. In this chapter, we only discuss the pseudonym technologies.

Pseudonym Technology

> *"The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."*
>
> -- U.S. Privacy Protection Study Commission, 1977

With the characteristics of unlinkability, anonymity, and accountability, pseudonym technology has become available after lengthy research. The technology for pseudonym systems took a major step forward with the introduction of digital pseudonyms. According to a high-tech dictionary definition, a digital pseudonym is a pseudonym an individual can use to set up an online account with an organization without revealing personal information. For instance, a public key, which is owned by an anonymous holder, can serve as a digital pseudonym. The holder can prove s/he is the owner of the public key by verifying signatures made with her/his corresponding private key. Digital pseudonyms were first introduced by David Chaum (Chaum, 1981) in 1981 for untraceable electronic mail services. In this system, an authority creates a roster for all pseudonyms and decides which applications of pseudonyms to accept but the authority is unable to trace the pseudonyms in the roster. The technology aimed at providing some limited anonymity for MIX networks which can take a

list of values as input and outputs a permuted list of function evaluations of the input items without revealing the relationship between input and output elements.

The concept of pseudonym systems was introduced by Chaum in 1985 (Chaum, 1985) in order to protect the privacy and maintain the security of both individuals and organizations for large-scale automated transaction systems. Pseudonym systems have several features. First, they allow users to interact with multiple organizations anonymously using pseudonyms so that personal information is not required or used for identifying themselves. For example, a purchase with e-cash is made under a one-time-use pseudonym credential. Second, with the pseudonym technology an individual is able to authenticate ownership of the pseudonyms and ensure that the pseudonyms are not improperly used by others. Furthermore, the individual can obtain a credential from one organization using one of her/his pseudonyms and demonstrate possession of the credential to another organization without revealing her/his first pseudonym to the second organization. For instance, a consumer may get e-cash from her/his bank and make a purchase with it in any retail store. In the pseudonym systems, an individual uses a different digital pseudonym with each organization. These pseudonyms are unlinkable to the person's identity, but the organizations are able to ensure that the pseudonyms are not used improperly.

In order to give a practical implementation for pseudonym systems, Chaum and Evertse developed a model and constructed a scheme in 1986 (Chaum & Evertse, 1986) based on the RSA public key cryptosystem (Rivest et al., 1978). In this scheme, the credentials are the RSA signatures on pseudonyms. However, the

disadvantage is that the scheme relies on a trusted central authority who must sign all credentials.

Damgard presents another pseudonym system scheme in 1988 (Damgard, 1988) based on a multiparty computing protocol with secret inputs and outputs. The scheme is to establish the existence of credential mechanisms, protect organizations from credential forgery, and secure the secrecy of users' identities at an information-theoretic level, i.e. unconditionally secure (Menezes et al. 1996). In addition, the role of the central authority in this scheme is limited to ensuring that each pseudonym belongs to the valid user.

In order to simplify the process of validating pseudonyms, Chen shifts the credential system from an RSA setting to a discrete logarithm setting (Chen, 1995). In this scheme, the central authority will no longer be required after the pseudonyms are validated since each organization has its own secret key for issuing a credential without the central authority's help. In addition, users can validate their own secret keys in the system when the signatures are required under the pseudonyms. Another feature of this system is that each version of the credential can be shown only once to an organization which makes it suitable for one-time credential environments such as an electronic cheque.

The newest and most sophisticated pseudonym technology is Pseudonym Systems that have been proposed by Lysyanskaya, Rivest, Sahai, and Wolf (Lysyanskaya et al., 2000) based on discrete logarithms in order to prevent a user from sharing her/his pseudonyms or credentials with other users. In this model, each user could open her/his accounts with different organizations using different unlinkable

pseudonyms after s/he registers with a Certification Authority (CA). The organization then issues a credential to the user by the pseudonym which s/he uses to open the account. The credential could be single-use like an e-cash or multiple-use like a health card depending on the application.

Another new pseudonym technology is Private Credentials recently proposed by Zero-Knowledge Systems (Glenn et al., 2001; Brands, 2000). Private Credentials minimizes the risk of identity fraud and overcomes the efficiency and security shortcomings of identity certificates, especially beneficial in the authentication-based environment.

Finally, anonymous e-cash (Chaum, 1982, 1988), e-wallet (Chaum & Pedersen, 1992), e-ticket (Song & Korba, 2003), and e-voting (Liaw, 2003) are other state-of-the-art pseudonym technologies for privacy protection in e-services. As a variety of e-commerce and e-government services are becoming huge driving forces for the future of the Internet, these solutions offering privacy and anonymity protection are very valuable.

Challenges and Issues

The past few years have shown a significant increase in public privacy awareness along with the widespread use of the varied e-services. Some of challenges and issues associated with privacy protection for e-services are highlighted here.

- **Consumer Attitudes**

More and more consumers have realized the value of their personal information and the danger in leaving it unprotected. According to a multi-national privacy survey by IBM (IBM, 1999), 80% of US consumers strongly agree that they have lost all control over how their personal information is collected and used by companies, and 54% of consumers have decided not to purchase anything from a company when they are not sure how the company will collect and use their personal information. Furthermore, privacy breaches almost always result in a decrease in customer loyalty and cause damage to the reputation of the e-services.

- **Legislation**

Governments around the world are beginning to introduce more and more privacy regulations and legislation for personal information protection. Some of them have become law, for instance, the European Union Directive on Data Protection (European Union), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada), and the U.S. Health Insurance Portability and Accountability Act (HIPAA) (U.S. Government). There are many challenges when enacting privacy programs, for instance, the organizations must not only be aware of current regulations but also strategically plan for future regulations. In addition, the companies must monitor the regulatory environment, create privacy standards and documentation, establish office procedures, and train their employees.

In order to spell out the requirements for the collection, use, disclosure, retention, and disposal of personal data, Canada has incorporated 10 Privacy Principles

(Dept. of Justice) in PIPEDA. However, the implementation of the principles may vary in the different systems due to different underlying applications.

- **Public Safety**

Public safety is another challenge for privacy protection. Citizens have been forced to question how much they value their personal information compared to their safety after the terrorists attacks on the U.S.A. in September 11, 2001. Consequently, public tolerance to surveillance has increased. New legislation has been passed to make the citizens' personal information more accessible to those who require it (e.g. police) in order to fight terrorism. However, this also allows personal information to be more accessible to those who shouldn't have access if the precautions or technologies are taken inappropriately. It is a significant challenge to satisfy the requirements from both privacy protection and public safety.

- **Technology**

Advancements in information technologies such as the Internet, high speed transfer, packet sniffing technologies, and efficient data mining have made personal data collecting, transmitting, storing, and analyzing much easier than before. It is becoming harder and harder for consumers to protect their personal data.

As a good privacy protection technology, pseudonym technology has many advantages such as anonymity, authenticity, and accountability. However, there

are many challenges as to how to make the pseudonym technologies satisfy the privacy requirements and principles within the varied e-services and how to make them comply with privacy legislation and standards. Other issues may arise from the trustability, reliability, and practice of a privacy protection system.

In addition, a good privacy protection system may require many privacy protection mechanisms and technologies to be used together since each of them has limitations. For instance, pseudonym technology usually has limitations when defending against traffic analysis (see Raymond, 2000) and may need other technologies such as onion routing (Goldschlag et al. 1999) and MIX networks (Berthold et al. 2000).

PSEUDONYM SYSTEMS

In order to have a good understanding how a pseudonym system can protect a user's privacy in e-services, we first summarize the pseudonym requirements for privacy protection in e-services. We then introduce a general pseudonym system architecture and discuss its relationship with other privacy technologies.

Pseudonym Requirements for E-Services

Privacy protection requires that each individual has the power to control her/his personal data, for instance, deciding how her/his personal data is collected and used. In order to do this, some privacy requirements have been researched by Brands and Lysyanskaya (Brands, 2000; Lysyanskaya et al., 2000). However, to comply with as many of the privacy principles and legislation as possible and to

improve e-services, a good pseudonym technology should satisfy the following characteristics.

Basic Requirements: These are very important requirements for a pseudonym technology in order to satisfy the privacy principles and be applicable to e-services. We say they are basic because anyone of them, if broken, can destroy the whole system. Furthermore, we categorize them as privacy-related requirements and security-related requirements.

Privacy-Related Requirements:

- **Pseudonymity**: Pseudonymity can let the user maintain one or more persistent personae but these personae are unlinkable to the user's physical identity. This allows a pseudonym to have a certain level of anonymity in order to serve as a basic requirement for privacy. As many researchers have already addressed, full anonymity is not beneficial to anyone under many situations, especially authentication-based e-services. With pseudonymity, the users can control their personal data more effectively. In addition, it is of great benefit to organizations, too. They can minimize the risk of identity fraud, increase the authenticity and accountability of their e-services, and cultivate goodwill among users.
- **Unlinkability**: Unlinkability means that the organizations cannot learn more than what the pseudonym reveals, i.e. to make the pseudonyms linkable is not much better than random guessing. This requirement can let the users control

how much personal data they actually disclose under an e-service. Otherwise, the aggregate linked information would be much more than the users were willing to disclose.

- **Property sharing resistance**: This is to protect organizations from a user that improperly shares her/his pseudonyms or credentials with other users so that the users can get some privileges which they otherwise would not have. It is very difficult to reach this goal for a protocol, especially for multiple-use credentials. There are two solutions to-date. One is to let the credential sharing become like e-cash sharing (the e-cash system checks for double-spending). This at least causes the organization no big loss. The other solution is to let the pseudonym or credential sharing result in sharing the user master secret key such as in the Pseudonym System (Lysyanskaya et al., 2000) and the Private Credential (Brands, 2000) (detailed information in the next Section).

Security-Related Requirements:

- **Authentication**: With authentication, the organizations can authenticate the users effectively, i.e. reject the invalid users or hackers and accept the valid users only. This is a basic security requirement for most e-services.
- **Unforgeability**: Unforgeability requires that a credential cannot be generated solely by the user. It must be issued with the organization's cooperation. Without unforgeability, the system will become useless.
- **Security of the user's secret key**: The system must make sure that the user's secret key is not revealed during all system processing. In addition, the key

generation technology itself should make sure that the secret key is secure under complexity-theoretic security or computational security.

- **Security of the protocols**: All security protocols in the system must be strong enough under existing cryptanalysis technologies and secure against the varied attacks.

Advanced Requirements: These requirements are considered secondary for a pseudonym technology since they are only adding more features for a pseudonym technology and some pseudonym applications may not require them. But they add very good properties to some special application systems and make the technology work more effectively for certain special e-services.

- **Selective disclosure**: This means that the user can show the different attributes of a credential to the different organizations without revealing other attributes in the credential. One example is Private Credentials proposed by Brands (Brands, 2000). This is a very good property for most multiple-use credentials.
- **Reissuance**: This requirement was also proposed by Brands. With this property, an organization can refresh an issued credential without knowing the attributes it contains. The technology can prevent the organization from learning attributes of the credentials. In addition, different organizations can certify different attributes for the same credential that has this reissuance property.

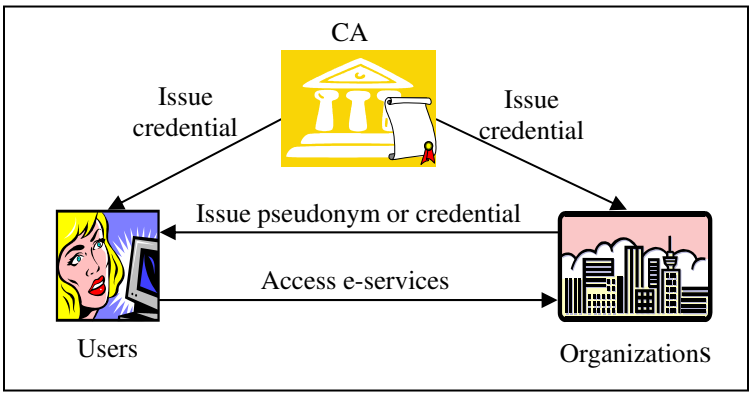
- **Dossier resistance**: This is another requirement presented by Brands in order to let a multiple-use credential leave no more evidence that it is necessary to validate the user at the transactions. One solution is to use a self-authenticating technology to let the credential have self-authenticating evidence for user validation. This requirement can protect the users against a central authority learning more personal information than the users have disclosed.
- **Non-repudiation**: With this requirement, the system can protect the organizations against a user denying her/his previous actions. Most of the pseudonym technologies use signature technologies for non-repudiation services but the signature does not reveal any personal information about the user (Song & Korba, 2003).
- **Confidentiality**: This protects the content of information such as the communication messages or credential's attributes from all but the users or organizations authorized to have them. With this requirement, the pseudonym technology has to use some encryption and decryption algorithms.

Pseudonym System Architecture

A pseudonym system is an identity and certificate management system with pseudonym and credential management and privacy protection functionalities. It consists of three parts: certification authority, organizations, and users, based on the pseudonym architecture models developed in Chaum & Evertse (1986), Chen (1995), Lysyanskaya et al. (2000), and Brands (2000). The certification authority

(CA) is a special organization to register users and organizations with their public keys and issue the public key credentials to them as the valid users and organizations in the system. Users can then prove to an organization that their pseudonyms correspond to the public keys of the valid users. The organizations (e.g. bank, government) set up pseudonyms and accounts for the users to access their e-services. Some organizations may issue private credentials to the users so that the users can demonstrate possession of the credentials to other organization without revealing their personal information. Each user uses different pseudonym accounts with different organizations and the pseudonym accounts are unlinkable to each other. Figure 1 depicts the components of a general pseudonym system and the process flows among the different components.

Figure 1. General pseudonym system components



A fundamental technology used in most pseudonym systems is the blind signature technology. In a pseudonym system, to register her/his pseudonym with an organization, the user must show her/his real name or certificate to the organization for verification. In order to avoid the organization to trace her/his pseudonym, s/he usually creates a blinded pseudonym message (using a specially designed function with the pseudonym and a random number as input) and sends it for registration. After verification, the organization signs the blinded pseudonym message and sends it to the user. The user then employs the organization's signature together with her/his pseudonym to access the organization's services. The organization cannot trace the pseudonym since the signature of the pseudonym is different from the organization's signature of the blinded pseudonym message.

The above pseudonym system involves several different public keys, for instance, master public key, pseudonym, and credential. These keys are issued by different organizations and have different purpose. Table 1 gives a simple comparison of them.

Table 1. Comparison of the different keys in a pseudonym system

Features / Keys	Key Generating Party	Key Issuer	Key Generating Protocol	Protocols where Key Applied
Master public key	By user	CA	Registration protocol	All protocols in the system
Pseudonym	By user and organization	Organi-zation	Pseudonym registration protocol	Pseudonym authentication protocol
Credential	By user and organization	Organi-zation	Credential issue protocol	Credential transfer protocol

- **Master public key**: The concept of the master public key was proposed by Lysyanskaya (Lysyanskaya et al., 2000) in order to protect the pseudonym system against property (pseudonym and credential) sharing. This means that the user must share her/his master secret key with others if s/he wants to share pseudonym or credential with them in the pseudonym system. To do it, a set of special protocols should be designed carefully. The user can generate her/his pseudonyms or credentials with the organization together using her/his master public key and secret key by running the protocols. In addition, the user must register her/his master public key with the certification authority first in order to make the master public key valid in the system. In some pseudonym technologies like e-cash, the user doesn't have a master public key. In that case, the user usually uses her/his public key certificate to get the pseudonym or credential (e.g. e-coin) by running a special protocol (e.g. blind

signature protocol). The credential (e-coin) sharing here is sharing their money.

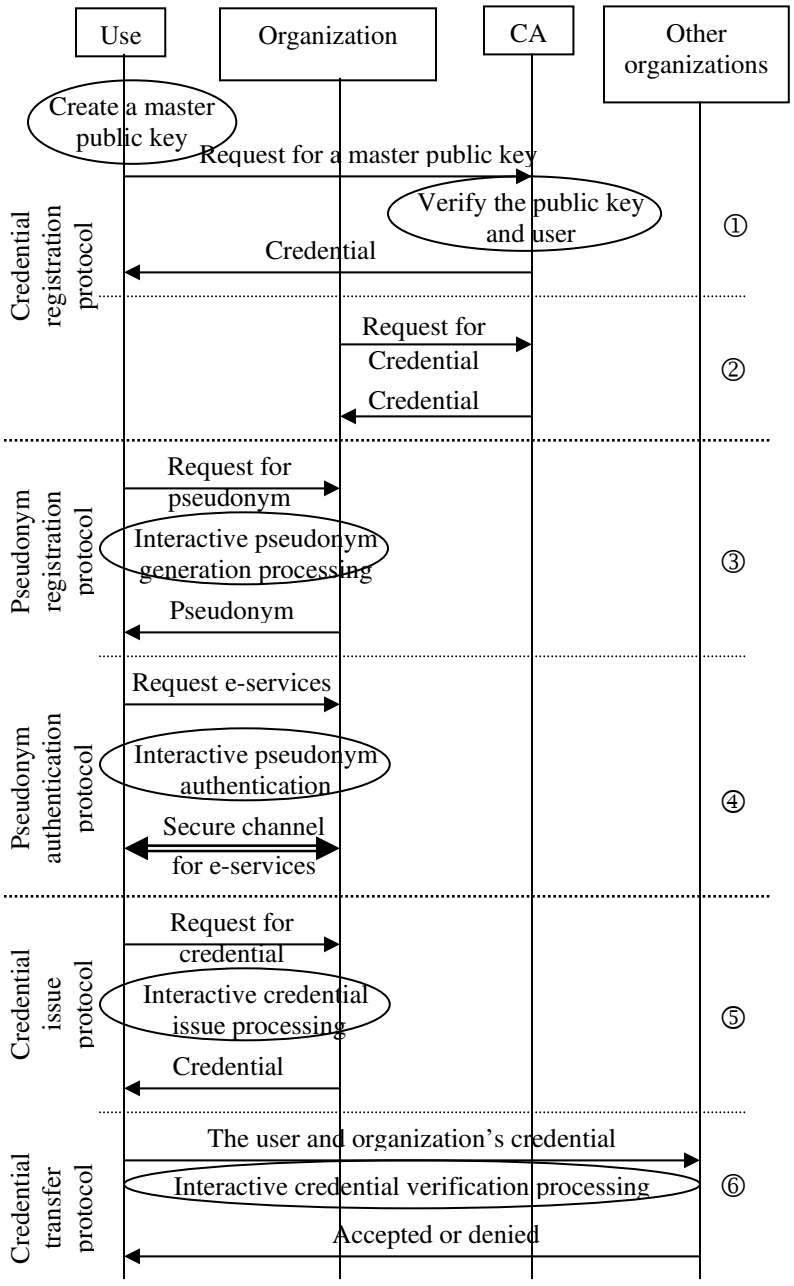
- **Pseudonym**: A pseudonym is one kind of public key which has the same secret key as the master public key if the system uses the master public key technology. The pseudonyms are issued by the organizations for their clients to access their e-services anonymously and authentically. Another purpose of the pseudonym is to generate a credential for the user using the organization's interactions. In order to get a pseudonym, the user must interact with the organization by running a pseudonym generation protocol with her/his master public key and secret key.
- **Credential**: A credential is one kind of certificate. Some schemes use the same secret key with the master public key and pseudonym for the credentials during authentication, for instance, Lysyanskaya's scheme (Lysyanskaya et al., 2000). Other schemes use different secret keys for each credential such as e-cash and e-ticket (Song & Korba, 2003). The credential is usually issued by one organization to a client of the organization to demonstrate to another organization that s/he has gone through credential issuance. A good example is that a bank issues e-cash to a client and the client gives the e-cash to a retail store for purchasing some products. In order to get a credential, the user must interact with the bank by running a credential issue protocol with her/his pseudonym and secret key.

The following protocols should be designed and developed in a pseudonym system in order to reach the above goal and complete the privacy protection functionalities. Figure 2 depicts the work flow of the protocols in a pseudonym system, where the longer dotted line separates the different applications, the shorter dotted line separates the different protocols under the same application based on the process sequence, and the ellipses represent activities made by a subject if the ellipses are under the subject directly, or interactive activities made by two subjects if the ellipses are between the two subjects.

- **The user master public key registration protocol**: The goal of this protocol (shown in part ① of Figure 2) is to issue a credential to a user based on her/his master public key so that s/he can prove to an organization that s/he is a valid user who owns the master public key in the system. In this protocol, the user is required to reveal her/his true identity and master public key to the certification authority. The certification authority verifies if the user really owns the corresponding secret key of the master public key by an interactive security protocol, for instance, a challenge-response authentication protocol. If the verification is successful, the CA will issue the corresponding credential of the master public key to the user.
- **The organization credential registration protocol**: This protocol (shown in part ② of Figure 2) is to issue a credential to an organization. The procedure of the protocol is similar to the previous protocol. With the public key credential an organization can prove to users or other organizations that it is a valid organization in the system.

- **The pseudonym registration protocol**: In this protocol (shown in part ③ of Figure 2), the user first sends her/his master public key and corresponding credential to the organization. The organization will generate a pseudonym for the user with the user together through a pseudonym generation protocol and open a pseudonym account for the user to access the e-services.
- **The pseudonym authentication protocol**: The pseudonym authentication protocol (shown in part ④ of Figure 2) establishes a secure communication between the user and organization. It could be a normal authentication with pseudonym characteristics. The user must prove that s/he is the owner of the pseudonym during authentication. After the protocol, a secure communication channel should be established between the user and organization.
- **The credential issue and transfer protocols**: The goal of these protocols is to let a user obtain a credential from one organization using her/his pseudonym and prove possession of the credential to another organization without revealing any other personal information about herself/himself. In these protocols, the user needs to prove that s/he is the owner of the pseudonym first by running a pseudonym authentication protocol. The organization then interacts with the user together and generates a credential for her/him through the credential issue protocol (shown in part ⑤ of Figure 2). After that the user can demonstrate to another organization that s/he is the owner of the credential through the credential transfer protocol (shown in part ⑥ of Figure 2).

Figure 2. Work flow of the protocols in a pseudonym system



Practice and Relationship with Other Privacy Technologies

As we mentioned, there are several kinds of privacy protection techniques for e-services. They have different functionalities. The main purpose of pseudonym technology is to provide anonymous authentication for users to access e-services. With pseudonym technology, a service provider can verify the users through access control but the provider cannot link the pseudonyms with the real identities of the users. The technology can limit the provider's ability for personal information collection. The pseudonym technology should be implemented as part of the access control and identity management in an e-service system. Obviously, it cannot protect the users from traffic analysis attacks during communications. For instance, a service provider or an attacker can easily trace a computer with some Meta Data such as IP address in the communication network layer and link the pseudonym used in the communication with the user of the computer. Anonymous communication networks such as onion routing or MIX networks can provide anonymous communication for users to protect their privacy from traffic analysis attacks in the communication layer, such as tracing a message to identify the sender and receiver. With this technology, it is very difficult for a service provider to trace the real source or destination of a message, but it cannot prevent the service provider from collecting personal information through the communication content if the system does not use other privacy mechanisms such as pseudonym technology. Privacy policy technology refers to efforts to protect

the user's privacy by controlling the personal data with certain rules which are compatible with privacy legislation. For a service provider, the rules may describe which part of personal information it will collect and for what purpose. In a policy enforcement system, some rules may trigger security mechanisms such as encryption and integrity in order to protect the personal data.

Usually, pseudonym technology is provided by an e-service provider and implemented in the application layer along with the e-service system. The anonymous communication network is provided by an anonymous network service provider and implemented in the lower communication network layer. Obviously, anonymous communication and pseudonym technology are implemented separately. However, they can be easily combined and used together in order to provide solid privacy protection for an e-service system. For instance, in a Web-based service system, a user can set up http communications through an anonymous network proxy and let the anonymous network forward her/his communication messages. S/he can then use her/his pseudonym, which is provided by a service provider, to access the Web service. This is not difficult for a person who has the required knowledge. Less knowledgeable users, however, may feel incapable of managing these technologies. A privacy policy enforcement system can provide efficient methods and give the user a better understanding of privacy protection. Such a system can combine these technologies together so that the user only has to manage her/his privacy policy. The policy will automatically call the privacy and security mechanisms to protect privacy.

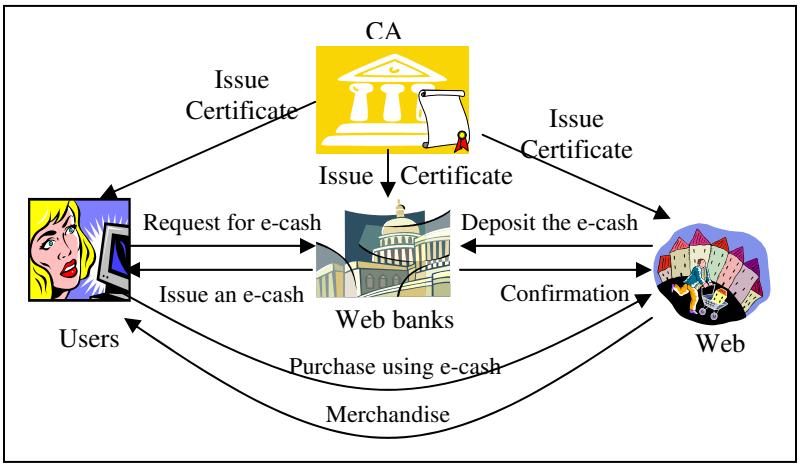
PSEUDONYM TECHNOLOGIES FOR E-SERVICES

We review several pseudonym technologies for privacy protection in e-services in this section and compare them based on the pseudonym requirements listed above. These pseudonym technologies are E-cash, E-ticket, E-voting, Pseudonym System, and Private Credentials.

E-cash System for E-commerce

Electronic cash (e-cash) is a kind of digital money which can be transferred by means of a computer network and traded as a token exchangeable for real money (Telecom Glossary 2000). In pseudonym systems, e-cash is one kind of single-use credential. The e-cash system was first proposed by Chaum in 1982 (Chaum, 1982; Chaum et al., 1988) in order to protect personal information from payment tracing by using a blind signature technology (explained below). After that, many new e-cash schemes have been proposed and developed with improved properties, for instance, Abe's scheme (Abe & Fujisaki, 1996), Miyazaki's scheme (Miyazaki & Sakurai, 1998), and Kim's scheme (Kim & Oh, 2002), but blind technology is always the key technology used to achieve the privacy protection goals for e-cash systems. Figure 3 depicts an e-cash system.

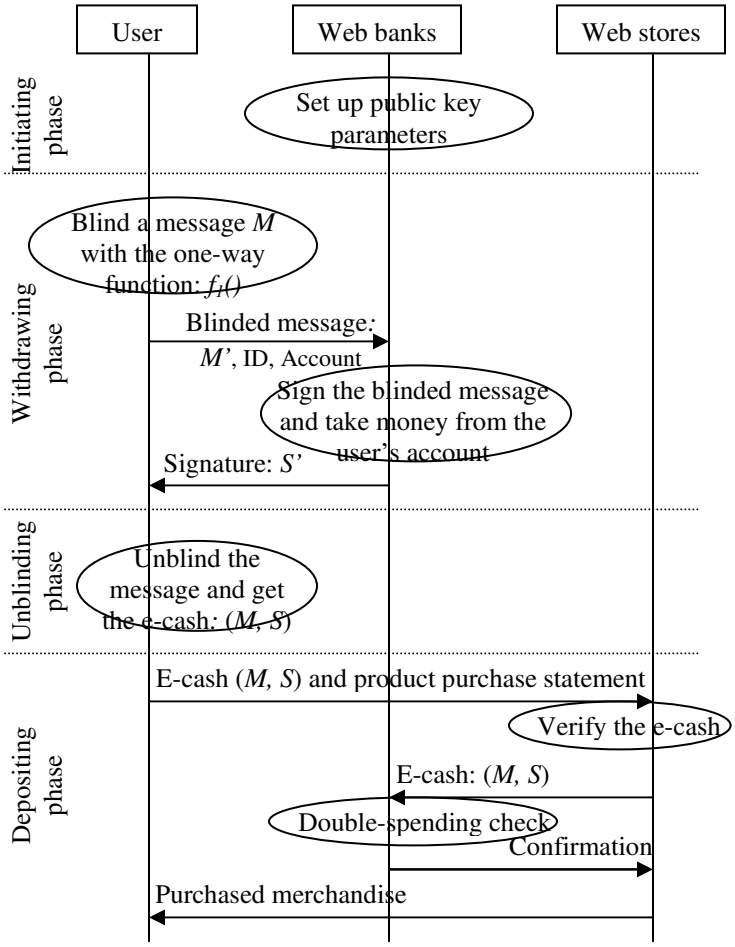
Figure 3. E-cash system components



An e-cash system consists of four elements: a certification authority, Web banks, Web stores, and users. The certification authority issues the public key certificates to the users, Web banks, and Web stores. In the system, the principal technology used is the blind signature technology involving four phases. The first phase is the initiating phase. In this phase, the bank will set up its public key parameters for the e-cash system. The second phase is the withdrawing phase. In this phase, the user requests to withdraw e-cash from her/his bank. To do this, the user blinds a message (M) that contains a random number as pseudonym using a specially designed one-way function (e.g. $f_1()$), i.e. the blinded message is $M'=f_1(M, r...)$ where r is a secret random number (pseudonym) owned by the user. The user then sends the blinded message (M') with her/his identity and bank account to the

bank. The bank signs the blinded message (*M'*), takes the money for the e-cash from the user's account, and sends the signature (*S'*) to the user. The third phase is the unblinding phase in which the user recovers the bank's signature (*S*) on the original message (*M*) using another one-way function (e.g. $f_2()$), i.e. $S = f_2(S', r...)$, and gets her/his e-cash (*M, S*). We call this mechanism a blind signature. It means the bank cannot trace back to the user when the user spends (*M, S*) later. The last phase is the depositing phase. In this phase, the user can buy any merchandise in a Web store with the e-cash. The Web store will verify the e-cash and send it to its Web bank for an online or offline double-spending check. If the double-spending check is successful, the bank will add the same money to the store's account. The store then delivers the purchased merchandise to the user. Figure 4 (CA's function not shown) depicts the system processing work flow.

Figure 4. Work flow of an e-cash system



E-cash is a single-use credential but its pseudonym uses a random series number, not a public key, so that the user usually doesn't have a secret key for the user authentication. This forces the system to use other technologies such as SSL for the user authentication. Furthermore, the system uses a double-spending check technology in order to resist property sharing. A good e-cash system satisfies

most of the pseudonym requirements such as pseudonymity, unlinkability, unforgeability, property sharing resistance, dossier resistance, and security of the protocols, but it doesn't have characteristics like authentication, selective disclosure, reissuance, non-repudiation, and confidentiality, where the authentication and non-repudiation are very important requirements for an e-commerce application. Most real applications use SSL technology for the user authentication. This would expose the user's identity and destroy the unlinkability. One solution we suggested is to embed a public key into the e-cash as the pseudonym instead of the random series number (Song & Korba, 2004). The main idea is similar to the following e-ticket system.

E-ticket for Pay-TV System

Security and privacy on Pay-TV system have been researched for some time (see Lee et al., 2000; Lee, 2000; Song & Lyu, 2001; Song & Korba, 2003). The latest electronic ticket system (e-ticket) for Pay-TV applications was proposed by Song and Korba (Song & Korba, 2003). In this system, an e-ticket could be a single-use or multiple-use credential depending on the application requirements. The e-ticket technology is based on existing e-cash technology (Abe & Fujisaki, 1996) but it enhances the security and privacy characteristics with user authentication and non-repudiation protection for the system.

The system consists of three elements: certification authority, TV service providers, and users. The certification authority issues the public key certificates to the TV service providers and users. The TV service providers issue e-tickets to

the users. The users then use the e-tickets to subscribe to TV channels. The protocol for the system includes four phases as follows.

(1) E-ticket issue phase: In this phase, the user inserts a random public key as a pseudonym in the blinded message so that the user holds a secret key for the e-ticket. This enables the system to support the user authentication and non-repudiation protection when the user spends the e-ticket later.

(2) TV channel subscription phase: In this phase, the user sends a statement of the TV channels and programs along with her/his e-ticket to the TV service provider. The whole message sent to the provider from the user is signed with the corresponding secret key of the pseudonym by the owner of the e-ticket so that the provider can authenticate the message by the signature and time stamp. At the same time, the provider charges the money from the e-ticket and sends the balance to the user through an anonymous network or e-mail if the e-ticket is a multiple-user credential. Otherwise, the provider will destroy the e-ticket.

(3) TV channel adaptation and suspension phase: In this phase, the user can change and stop her/his selected TV channels. To do this, the user sends the changed information with the e-ticket together to the provider. The provider will authenticate the user by the signature.

(4) E-ticket renew phase: The user can renew her/his e-ticket before the e-ticket expires. To do this, the user sends her/his old e-ticket to the provider. The provider then reissues the e-ticket to the user with a new expiration date.

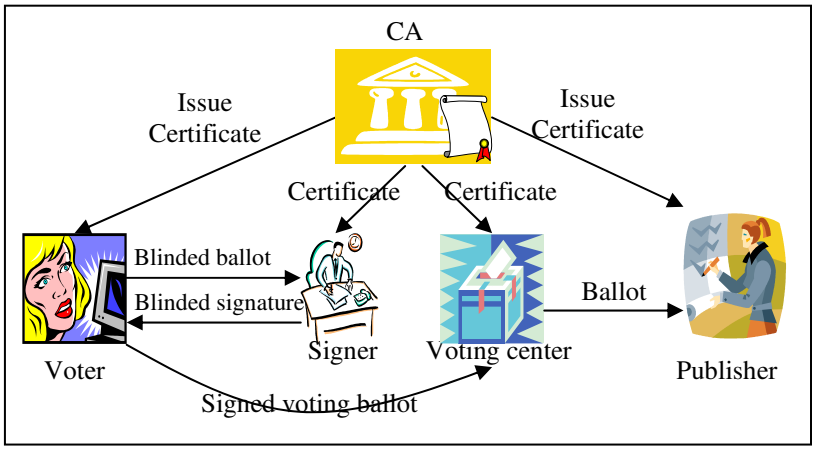
The e-ticket system satisfies all the pseudonym requirements that we mentioned above except selective disclosure. Selective disclosure is not required for a Pay-TV system. In order to satisfy sharing resistance, the system uses the double-spending check so that the pseudonym or credential (e-ticket) sharing means money sharing for the consumers.

E-voting

Electronic voting (e-voting) is an election system that allows voters to record their secure and secret ballots electronically. In the last 20 years, many kinds of e-voting technologies have been proposed and developed, for instance, Internet-based, telephone-based, anonymous network-based, and pseudonym-based (Chaum, 1988; Cramer et al., 1997; Hoffman, 2000; Jorba et al., 2003; Juang et al., 2002). Here, we only discuss pseudonym-based e-voting technologies. The latest pseudonym-based e-voting scheme was proposed by Liaw in 2003 (Liaw, 2003) to solve some problems such as uncoercibility, non-cheating, uniqueness, fairness, anonymity, mobility, and efficiency. This system consists of five elements: certification authority, publisher, decryptor, signer, and voters. The certification authority issues the public key certificates for the users, signer, and publisher. The signer will sign and check the voter's election anonymously using a blind signature technology. The voter then sends the signed voting ballot to the untraceable decryptor (renders voting ballot untraceable) in the voting center. The voting center records the voting ticket and forwards it to the publisher. The

publisher finally decrypts the voting ticket and reveals the voting result. Figure 5 depicts the e-voting system and process flow.

Figure 5. E-voting system components



In this system, an electronic ballot (e-ballot) is a single-use credential. The primary technology used in the system is a blind signature scheme. The protocol includes four phases: initiating phase, voting phase, scrutiny phase, and publishing phase.

(1) Initiating phase: In this phase, the signer, publisher, and voters request their public key certificates from the certification authority. In addition, each voter needs to request a smart card from the CA with a unique identifying number authorized by the CA. The smart card contains the signer's public key and

publisher's public key for computing the blinded voting message. For each vote, the voting center chooses a random number (RD) to check the validity of the votes. The random number is used to create the blinded voting message.

(2) Voting phase: In this phase, each voter fills out her/his voting ballot, and inputs it into her/his smart card. The smart card encrypts and blinds the ballot with the signer's public key, publisher's public key, and random number RD together, and sends it to the signer. The signer verifies the message and signs it for the voter. With this signed message, the voter obtains the signature for the blinded ballot. Finally, the voter sends the blinded ballot with the signature to the voting center.

(3) Scrutiny phase: The voting center verifies the signature and the blinded ballot. It then records the voting ballot and forwards it to the publisher if the verification is successful.

(4) Publishing phase: Upon reception of the voting ballot, the publisher decrypts the ballot and publishes the vote that consists of a hash number and a voting choice. The hash number was created by the voter with a random number in the voting phase so that the voter can use the published vote (both hash number and voting choice) to check if her/his vote has been counted.

This e-voting system satisfies most of the pseudonym properties listed above except for non-repudiation, selective disclosure, and reissuance. This is to be expected since e-voting has different requirements from other e-services such as e-cash and e-ticket. In addition, this e-voting system satisfies other properties

which are not listed in the above pseudonym requirements but are very important for an e-voting system, for instance, completeness, incoercibility, and non-cheating.

Pseudonym Systems

The general pseudonym system architecture has been described above. We now introduce a recent pseudonym system called Pseudonym Systems constructed by Lysyanskaya (Lysyanskaya et al., 2000). The system is based on a blind transcription technology, the discrete logarithm problem (Menezes et al., 1996), and the ElGamal public key cryptosystem (ElGamal, 1985).

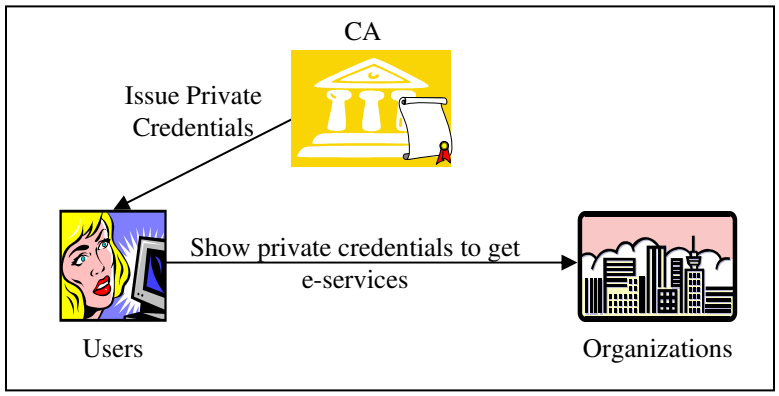
In this system, the users first set up their master public key parameters, publish their public keys through a Public Key Infrastructure system (PKI) or others and keep the secret keys for themselves. Each organization creates their credential keys for issuing pseudonyms. After that, a user can apply the different pseudonyms from the different organizations for their e-services, where all pseudonyms are related to the user's master secret key in order to dissuade the user from sharing his/her pseudonym with others (which would result in the user sharing his/her master secret key). Using a pseudonym, the user can communicate with an organization securely and anonymously, for instance, through authentication, encryption, and signature. In addition, the user can apply credentials from organizations and use them with other organizations through the credential issue and transfer protocol, where the credentials also use the same secret key with the user's master public key for user authentication.

The system satisfies most of the pseudonym requirements listed above except for selective disclosure and reissuance.

Private Credentials

The Private Credentials system is an application proposed by Brands in 2000 (Brands, 2000) for the Freedom Network managed by Zero-Knowledge Systems. The primary technology in the Private Credentials system is similar to that of blind signatures first proposed by Chaum (Chaum, 1982; 1985). However, this technology has very different properties. For instance, Private Credentials has selective disclosure characteristics. In addition, the system has similar components as the pseudonym system shown in Figure 1. However, the process flows are very different. In the Private Credentials system, the certification authority directly issues the Private Credentials to the users. The users then show their private credentials to other organizations to get the e-services. Figure 6 depicts the process flow of the system.

Figure 6. Process flow of the Private Credential system



Two protocols – the private credential issue protocol and the authentication protocol – are designed and developed in order to promote practicality and simplicity (see Glenn et al., 2001). The protocols are patented by Zero-Knowledge Systems Inc.

- **Private credential issue protocol**: This protocol includes four phases. The first phase is the Initiating Phase. In this phase, the user and CA set up their parameters for issuing private credentials. The second phase is the Private Attributes Validation Phase in which the user must send all credential attributes to the CA. The CA verifies if these attributes are correct. The third phase is the Blinding and Signing phase. In this phase, the user blinds her/his pseudonym and credential with the parameters sent from the CA, and sends the blinded message to the CA. The CA then signs the blinded message and sends the signature to the user. The last phase is the Unblinding Phase in which the user unblinds the signature and gets her/his private credential. The private credential has two parts: public part like a pseudonym and secret part for authentication later.

  In this protocol the CA cannot learn who obtains which credential since the pseudonym (i.e. the public parameters of the credential) is blinded during the protocol.

- **Private credential authentication protocol**: With a private credential, the user can convince other organizations that s/he possesses the credential and use the corresponding secret key to authenticate a message.

Private Credentials satisfies almost all pseudonym requirements listed above. It uses the same strategy as Pseudonym Systems for discouraging property sharing, i.e. the property sharing will reveal the user's master secret key. In addition, Private Credentials has another good property - selective disclosure which makes the system more practical and convenient. For example, the user may want to disclose only his/her medical condition to a medical office instead of all private information. Many other pseudonym technologies don't have this property.

Comparison of Pseudonym Technologies

Based on the above review of the different pseudonym technologies and pseudonym characteristics, a comparison of them is presented in Table 2. The comparison only gives a general idea. In Table 2, an application that has more properties does not necessarily have better privacy protection since each application may have different requirements. For example, the requirements for the e-voting system are very different with other applications like e-cash. In addition, the following comparison is based on the current techniques implemented or proposed. Pseudonym technologies for e-services are improved over time.

Table 2. Comparison of the different pseudonym technologies

Properties	E-cash	E-ticket	E-voting	Pseudonym Systems	Private Credentials
Pseudonymity	✓	✓	✓	✓	✓
Authentication		✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓	✓
Unforgeability	✓	✓	✓	✓	✓
Security of the secret key	✓	✓	✓	✓	✓
Security of the protocols	✓	✓	✓	✓	✓
Property sharing resistance	✓	✓	✓	✓	✓
Selective disclosure					✓
Reissuance		✓			✓
Dossier resistance	✓	✓	✓	✓	✓
Non-repudiation		✓		✓	✓
Confidentiality		✓	✓	✓	✓

CASE STUDY: E-WALLET

Current payment systems using credit card and bank debit card make it easy for the merchants to collect the consumer's personal data. They can easily record the user's purchase habits and personal information (e.g. the size of clothes purchased) during payment since the user's identity is on the card. The electronic wallet (E-wallet) provides a way to spend money and receive marketing material or services from service providers, and at the same time protect the consumer's privacy and payment transactions. With the e-wallet protocol (Chaum & Pedersen, 1992), users can obtain their pseudonyms (or credentials) to which the

issuer and other powerful organizations cannot link the users' identities. Unlike on-line e-cash, e-wallet can provide off-line payments (e.g. The ESPRIT Project CAFE (Boly, et al., 1994)). In order to examine how the e-wallet system can protect the user's privacy and secure payment transactions, we review its architecture and protocols, and introduce an application: the CAFE project. Finally, we discuss the current applications of e-wallet over the Internet.

E-wallet System Architecture

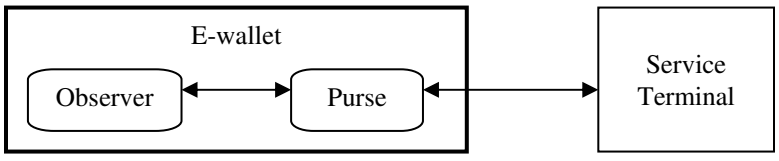
The electronic wallet was first proposed by Chaum and Pedersen (1992) in order to be sure that an organization can only store, read, and update valid information (e.g. pseudonym or credential) in a tamper-proof device (e.g. smart card) issued to a user. For these purposes, an e-wallet consists of an observer and a purse.

- The observer is the tamper-proof device (e.g. smart card) trusted by the issuer (e.g. bank) and protects the issuer's interest during off-line payment transactions. It is a container for e-coins issued by banks. However, the observer cannot directly communicate with service providers (e.g. retail stores or bank) during transactions. All communications from the observer must go through the purse to connect with outside (e.g. a service terminal).
- The purse is a hardware device owned and trusted by the user. When a user wants to spend her/his e-coins, s/he puts her/his observer into her/his purse and connects the purse to the service device using a standard interface. With the purse, the user can fully control the communications between the observer and service provider and this prevents the observer from performing

unsolicited actions. However, the user cannot modify the data stored in the observer nor can the user modify the transaction messages between the observer and service provider since the observer is a tamper-resistant device and the messages are protected by security functions such as digital signature.

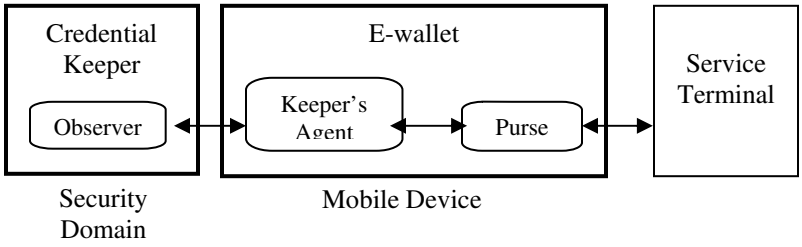
Figure 7 depicts the Chaum-Pedersen e-wallet architecture. From the architecture, we can see that the user (purse) can freely communicate with the outside world without the knowledge of the observer, but an honest organization (service terminal) will only accept messages approved by the observer. In addition, an e-wallet system is similar to an e-cash system (see Figure 3) but the e-wallet system can provide off-line payments (i.e. both the payer and payee do not need to connect to any bank during transactions) and better protections for both the consumers and service providers. For e-wallet applications, the European Community's ESPRIT project CAFE (Boly, et al., 1994) has developed technology and a generalization of the concept of an electronic wallet based on the security architecture of the Chaum-Pedersen e-wallet.

Figure 7. Chaum-Pedersen E-wallet Architecture



In order to make the e-wallet system work under the wireless and ubiquitous computing environment, Mjolsnes and Rong (2003) extended the system with decentralized credential keepers. In the Mjolsnes-Rong e-wallet system, the observer is located on the remote home security domain or on at a trusted third party named "credential keeper", like a bank safety-deposit box that stores and protects the pseudonyms and credentials issued to the user. The e-wallet is a mobile device (e.g. cell phone, PDA) and consists of the keeper's agent and a purse. The keeper's agent is a tamper-resistant hardware such as smart card that contains a secret key to protect the communications and transactions between the credential keeper and the agent. The credential keeper's agent is triggered to control and communicate with the credential keeper when the e-wallet application (purse) is required to communicate with the observer, for instance, to request a credential. Since the communications between the mobile device, credential keeper, and service terminal may cross an open public network, some end-to-end security protection mechanisms (e.g., AES end-to-end encryption, SSL/TLS security for Web services, Bluetooth Security Model 3 for short range physical services) are required. In addition, the Mjolsnes-Rong e-wallet system can be applied to various application areas such as the electronic acquisition of an e-token (e.g. e-ticket). Figure 8 depicts the Mjolsnes-Rong e-wallet architecture, where the service terminal can consist of physical services and Web-based services.

Figure 8. Mjolnes-Rong E-wallet Architecture

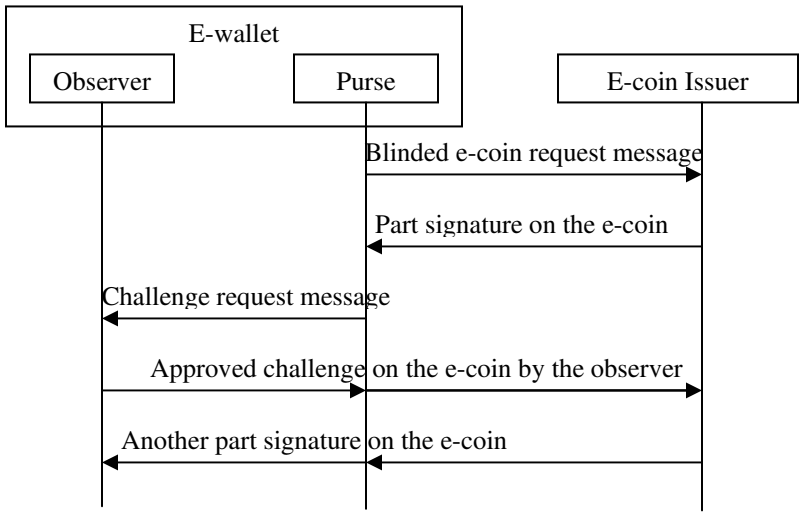


E-coin Issuing Protocol

In order to let the user ensure that her/his privacy is not compromised during transactions and let the observer validate all messages from the user to the outside world, Chaum and Pedersen designed an e-coin issuing protocol. The protocol is to avoid allowing the user to get a signature on any message that s/he chooses. For this purpose, the protocol must ensure that the message has been validated and approved by the observer before it is signed by the organization, i.e. the organization only signs the blinded message approved by the observer. However, the organization cannot learn any personal information from the blinded message although the observer knows the original message since the user (purse) only allow the observer to send the approved challenge to the outside organization if the user follows the protocol. Figure 9 concisely depicts the process flow of the protocol. With the protocol, a user can request an e-coin from an organization and store it into a smart card (observer). Later the user can show the e-coin to other

organizations, for instance, pay the e-coin to get a cup of coffee from a unsupervised and isolated coffee machine. With e-wallet, the user can use an off-line payment to pay for it, i.e. the user (purse) sends a message to the observer to record the transactions (e.g. deduct the e-coin from the smart card for the purchase) and get an approved payment transaction message from the coffee machine (e.g. a signature on the payment confirmation). Later, the owner of the coffee machine can get money from the bank using the e-coin and payment confirmation message stored in the coffee machine. However, with online e-cash, this off-line payment cannot be done.

Figure 9. E-coin issuing protocol in E-wallet



E-wallet Application Practice in CAFE

CAFE ("Conditional Access for Europe") is a European Community's ESPRIT project that is primarily intended for payments from e-wallet to POS (point-of-sale) and aims at a market of small everyday payments and personal data protection. In the CAFE system, every user has her/his own e-wallet, which controls her/his privacy and security.

The basic CAFE device is an electronic wallet based on the Chaum-Pedersen e-wallet security architecture. The e-wallet consists of two basic devices: a small portable computer (Purse) similar to a PDA (Personal Digital Assistant) and a tamper-resistant device (Observer) called Guardian. The purse protects the user's interests and the guardian protects the electronic money issuer's interests. In addition, the guardian is only allowed to communicate via the purse since the user is not supposed to trust the guardian. So the purse can check and modify all messages the guardian sends and receives. However, an honest payee only accepts the messages approved by the guardian on behalf of the payee, i.e. no payment is accepted without the guardian's cooperation such as a signature. In the CAFE system, the purse communicates with other outside devices such as service points and tills provided by banks and merchants using a short range infrared channel, or over a computer network such as the Internet. It can also directly make transactions with other e-wallets held by other users. In addition, the system can be combined with a PDA, mobile phone, or a laptop.

Except for the hardware devices (Purse and Guardian), CAFE also uses some cryptographic mechanisms such as blind signature and off-line coin to protect the

system. These crypto protocols can control all inflow and outflow of communications and prevent extra personal information from being disclosed to the outside world. With the blind signature protocols (Chaum, 1985, 1992), a CAFE user can obtain an electronic coin signed by an electronic money issuer but the issuer does not know what the electronic coin looks like except for a certain form that the electronic coin must take in order to be in compliance. This ensures that the electronic money issuer cannot recognize the coins when the payer spends them and thus be able to trace the payer. The off-line coin mechanism is designed for off-line payments (Chaum et al., 1988). With the off-line coin protocol, the payer's identity is encoded into the coin. The payer must reveal a part of the identity coded in the coin when he uses the coin for a payment. The protocol is constructed so that the identity can be found out if the same coin is used in two payments in which case the electronic money issuer can detect the cheating payers. More information can be found in (Chaum et al., 1988; Franklin & Yung, 1993; Brans, 1993). The CAFE system combines the off-line coin with the guardian in such a way that one part of the coin is held by the purse and another part by the guardian. The two parts together can create a secret key for signature on a payment with the electronic coin. The guardian can prevent an electronic coin from being spent twice because the guardian would know not to provide its part of the coin for the secret key twice.

Furthermore, CAFE employs a loss tolerance mechanism to protect the user from a wallet lost or stolen. The mechanism is based on the loss-tolerance electronic wallet proposed by Waidner & Pfitzmann (1990, 1991). The idea is to keep a

backup of the user's electronic money outside the wallet but the backup shouldn't violate the privacy of the payer and the security of the electronic money issuer. With the backup, the electronic money can be reconstructed and the part that has not been spent can be credited to the user's account.

Based on its security architecture, the basic CAFE system has implemented the following features.

- **Security**: The system uses the multi-party security mechanism (Chaum, 1985) which means the guaranteed security requirements do not force one party to trust other parties, i.e. a party has to trust itself and the jurisdiction. This is beneficial for all parties in the system. Furthermore, in the CAFE system, fake-terminal attacks can be prevented by directly entering PINs into the e-wallet during verification.
- **Privacy**: The system can protect the personal data with untraceability and unlinkability. This means that the payer (user) is perfectly untraceable for any payment transactions, i.e. the e-wallet issuer cannot learn the identity of the payer from the payment. Furthermore, the different payments are unlinkable.
- **Prepayment**: This means the user must purchase some electronic money from an electronic money issuer (e.g. bank) and store it into his e-wallet before he can make any payment transactions.
- **Off-line Payment**: It is not necessary to contact the electronic money issuer during a payment. This is good for low-value everyday payments since the on-line communication and processing with the electronic money issuer may be expensive for small payments.

- **Loss Tolerance**: This means that the user can get his money back if her/his e-wallet is lost, broken, or stolen.
- **Open Architecture and System**: This means that the system is designed for a universal payment system and interoperable between the different electronic money issuers. In addition, the system is open for new hardware platforms and can be integrated into other systems.

E-wallet Practice in Web-Based Services

E-wallet services and applications are becoming more and more popular on the Internet, especially for payments and transactions over the Internet. Many large Internet service providers such as Yahoo, Amazon, eBay, AT&T, and Microsoft, have provided e-wallet services. However, most of the e-wallet applications in current Internet services have lost the important functionalities of the original e-wallet such as pseudonym-based and owner controlled privacy protection, i.e. personal data can be protected with pseudonym technology and controlled by its owner with cryptographic technology such as the blind signature. These new e-wallet applications in Internet services use agreement–based and provider controlled privacy protection technology, i.e. the user's personal data is controlled and protected by the service provider, not the owner of the personal information, based on an agreement signed by the service provider and the owner (user). The agreement describes the conditions when and how the personal data can be used by the provider, exposed to whom, and for what purposes. For instance, the

AT&T Wireless e-Wallet User Agreement (2005) describes the privacy conditions of use of the AT&T wireless e-wallet as:

> *"We collect, and you consent to such collection of, the information you provide or confirm at registration as well as information about your purchases and other transaction information. We disclose that information, and you consent to such disclosure, to those merchants involved in the transaction, to your credit card company and bank, the merchant bank, merchant aggregators, and other vendors, companies or service providers used to facilitate or complete the transaction ("Third Parties"). Information about you received by those Third Parties will be governed by their own privacy policies, not this User Agreement or the AT&T Wireless Privacy Policy. Whenever third parties have a role in any transaction, you should review their privacy policies and practices. You consent to Third Parties sharing information about you with AT&T Wireless to facilitate e-Wallet transactions. In addition, you authorize AT&T Wireless and Payment Processor to exchange your registration and transaction information with each other in order to provide the Bill to Phone service to you."*

The personal information collected by AT&T is described in the AT&T E-WALLET SUPPLEMENTAL PRIVACY NOTICE (2005) as:

> *"In connection with the e-Wallet Services, we collect the following categories of personal information:*

Registration Information: We may collect personal information from you during the registration process, including: (i) your name and your mailing and email addresses, (ii) your mobile phone number, (iii) your credit card or debit card numbers, and (iv) a user name and password (PIN). AT&T Wireless also uses "cookies" to keep track of each use by you of e-Wallet Services, but does not store any information about you in a cookie.

Transaction Information and Information from Vendors and Merchants: We collect personal information about your use of the e-Wallet Services, including purchase and other information from your transactions conducted using the e-Wallet Services. This information may include the type of purchase, the name of the merchant, and the amount of the purchase. We also receive information from vendors or merchants that provide services either individually or jointly with us, as part of the e-Wallet Services or your other AT&T Wireless services."

This means the provider may collect a lot of personal information with the e-wallet services since the e-wallet uses the real name of the user for all payments and transactions. Furthermore, the e-wallet is a simple database that gathers personal information such as name, address, and credit card account, together with some security protection such as encryption. The major purpose of the e-wallet applications here is to provide a simple and convenient approach for payments and transactions in Internet services. Personal data protection relies on the privacy protection agreement and legislation.

FUTURE TRENDS

Pseudonym technology will be accepted and employed by more and more applications when people find that their personal information is readily exposed to the public. However, pseudonym technology needs to be improved and standardized in order to satisfy the requirements of the customers, applications, and legislations.

There is still much to be done in terms of pseudonym technology research for privacy protection in e-services. As we mentioned, most current e-services haven't applied pseudonym technologies since most of these technologies are still in the research stage. For instance, in e-commerce services, the current payment system and business model do not involve pseudonym technologies. It is a challenge to fill this gap and propose a practical pseudonym technology that can be easily combined with the current credit card or debit card payment system. CAFE is an example of a good practice towards answering this challenge. Furthermore, the computational complexity, efficiency, and scalability of the existing pseudonym technologies require further research to arrive at a state when they can be embedded in e-services. Lower cost, improved privacy protection, and better services are good drivers for the development of pseudonym technologies to achieve greater practicality. In addition, new e-services may require new pseudonym technologies to implement new privacy protection requirements required by organizations or the law.

In addition, along with the development of advanced technologies such as ubiquitous computing systems, wireless systems, high performance processors,

and large memory storage, a new kind of comprehensive e-wallet, which can contain thousands of different e-certificates, would become very attractive for e-services. More and more people are complaining that a small traditional wallet cannot take too many cards (e.g. credit cards, debit cards, driver license, and membership cards), and it is very dangerous and inconvenient if the traditional wallet is lost, since anyone can open the wallet when they find it. In this case, the thousands of e-certificates delegating the different physical cards can be easily stored into a small e-wallet. Compared with the traditional wallet, the e-wallet has many benefits, such as more security, large storage, more efficiency, and others. Of course, the new standards for the variety of e-certificates, e-wallets, and interfaces need to be researched and developed.

CONCLUSIONS

In this chapter, we have introduced the reader to current research, challenges, and issues of pseudonym technologies for privacy protection in e-services. We summarized the general pseudonym system architecture and processing of the protocols and gave a comparison of the different keys such as master public key, pseudonym, and credential involved in the system, including their functionalities and roles. We analyzed the pseudonym requirements for e-services and summarized them as two different kinds of requirements, i.e. basic requirements and advanced requirements, in order to evaluate the pseudonym technologies and applications. Furthermore, we reviewed several very important pseudonym technologies such as e-cash, e-ticket, e-voting, Pseudonym System, and Private

Credentials and compared them according to pseudonym properties. These technologies can be used in different applications and e-services to provide better privacy protection.

REFERENCES

Abe, M. & Fujisaki, E. (1996). How to Date Blind Signatures. *AsiaCrypto'96, LNCS 1163* (pp. 244-251).

AT&T Wireless e-Wallet User Agreement. (2005). *Available at http://www.mobile.att.net/e-wallet/agreement.html* searched in April, 2005.

AT&T E-WALLET SUPPLEMENTAL PRIVACY NOTICE. (2005). *Available at http://www.mymmode.com/e-wallet/privacy.html* searched in April, 2005.

Berthold, O., Federrath, H., & Kopsell, S. (2000). Web MIXes: A System for Anonymous and Unobservable Internet Access. *In H. Federrath (Ed.), Anonymity 2000, LNCS 2009*, (pp.115-129).

Boly, J. P., et al. (1994). The ESPRIT Project CAFE – High Security Digital Payment Systems. *Proceedings of Third European Symposium on Research in Computer Security (ESORICS 94), LNCS 875* (pp. 217-230).

Brands, S. (2000). Private Credentials. White paper by Zero-Knowledge Systems, Inc. *Available at: http://www.zks.net/media/credsnew.pdf.*

Brands, S. (1993). (1993). An Efficient Off-Line Electronic Cash System Based on the Representation Problem. *Centrum voor Wiskunde en Informatica, Computer Science/Department of Algorithmics and Architecture, Report CS-R9323*.

Chaum, D. (1981). Untraceable Electronic Mail, Return Address, and Digital Pseudonyms. *Communications of the ACM, Vol. 24, No. 2* (pp. 84-88).

Chaum, D. (1982). Blind Signatures for Untraceable Payments. In Chaum, D., Rivest, R. L., & Sherman, A. T. (Eds.), *Advances in Cryptology—CRYPTO'82* (pp. 199-203).

Chaum, D. (1985). Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM, Vol.28, No.10* (pp.1030-1044).

Chaum, D. & Evertse, J. (1986). A Secure and Privacy-protecting Protocol for Transmitting Personal Information between Organizations. *Advances in Cryptology—CRYPTO'86, LNCS 0263* (pp. 118-167).

Chaum, D. (1988). Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. *Advances in Cryptology—Eurocrypt'88* (pp.177-182).

Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable Electronic Cash. *Advances in Cryptology—CRYPTO'88* (pp. 319-327).

Chaum, D. & Pedersen, T. P. (1992). Wallet Databases with Observers. *Advances in Cryptology—CRYPTO'92, LNCS 0740* (pp. 89-105).

Chen, L. (1995). Access with Pseudonyms. In Ed Dawson and Jovan Galic (Eds.), *Cryptography: Policies and Algorithms, LNCS 1029* (pp. 232-243).

Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A Secure and Optimally Efficient Multi-Authority Election Scheme. *Advances in Cryptology—Eurocrypt'97, LNCS 1233* (pp.103-118).

Damgard, I. B. (1988). Payment Systems and Credential Mechanisms with Provably Secure against Adaptive Abuse by Individuals. *Advances in Cryptology—CRYPTO'88, LNCS 0403* (pp. 328-335).

Dept. of Justice. Privacy Provisions Highlights. *Available as of Feb. 28, 2005 at: http://canada.justice.gc.ca/en/news/nr/1998/attback2.html*

Diffie, W. & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, Vol. 22, No.6* (pp.644-654).

ElGamal, T. (1985). A Public-key Cryptosystem and A Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory, Vol. 22, No. 6* (pp. 469-472).

European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Unofficial text retrieved Sept. 5, 2003 from: http://aspe.hhs.gov/datacncl/eudirect.htm

Franklin, M. & Yung, M. (1993). Secure and Efficient Off-Line Digital Money. *Proceedings of 20th International Colloquium on Automata, Languages and Programming ((ICALP), LNCS 700,* (pp. 265-276).

Glenn, A., Goldberg, I.,Legare, F., Stiglic, A. (2001). A Description of Protocols for Private Credentials. White paper patented by Zero-Knowledge Systems, Inc. *Available at: http://crypto.cs.mcgill.ca/~stiglic/Papers/brands.pdf#search=' private credential'.*

Goldberg, I., Wagner, D., & Brewer, E. (1997). Privacy-Enhancing Technologies for the Internet. *IEEE COMPCON'97* (pp. 103-109).

Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion Routing for Anonymous and Private Internet Connections. *Communication of the ACM, Vol. 42, No. 2,* (pp. 39-41).

Government of Canada. Personal Information Protection and Electronic Documents Act. *Available as of Feb. 28, 2005 at: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp.*

Hoffman, L. J. (2000). Internet Voting: Will It Spur or Corrupt Democracy? *Proceedings of the 10th Conference on Computers, Freedom and Privacy: Challenges the Assumptions* (pp.219-223).

IBM. (1999). Multi-National Consumer Privacy Survey. *Available at http://www.mischiefmarketing.com/privacy_survey_oct991.pdf.*

Jorba, A. R., Ruiz, J. A. O., & Brown, P. (2003). Advanced Security to Enable Trustworthy Electronic Voting. *Proceedings of the 3rd European Conference on E-Government* (pp.377-384).

Juang, W. S., Lei, C. L., & Liaw, H. T. (2002). A Verifiable Multi-authority Secret Election Allowing Abstention from Voting. *Journal of Computer, Vol. 45, No.6* (pp.672-682).

Kim, S. and Oh, H. (2002). A New Electronic Check System with Reusable Refunds. *International Journal of Information Security, Vol.1, No.3* (pp. 175-188).

Lee, N. Y., Change, C. C., Lin, C. L., & Hwang, T. (2000). Privacy and Non-repudiation on Pay-TV Systems. *IEEE Transactions on Consumer Electronics, Vol.46, No.1* (pp.20-26).

Lee, N. Y. (2000). Fairness and Privacy on Pay-per View System for Web-based Video Service. *IEEE Transactions on Consumer Electronics, Vol.46, No.4* (pp.980-984).

Liaw, H. T. (2003). A Secure Electronic Voting Protocol for General Elections. *Journal of Computers & Security, Vol.23* (pp.107-119).

Lysyanskaya, A., Rivest, R. L., Sahai, A., & Wolf, S. (2000). Pseudonym Systems. In Howard Heys and Carlisle Adams (Ads.), *SAC'99, LNCS 1758* (pp. 184-199).

Menezes, A., Oorschot, P. V., & Vanstone, S. (1996). Handbook of Applied Cryptography. *CRC Press* (pp.103-113).

Miyazaki, S. & Sakurai, K. (1998). A More Efficient Untraceable E-cash System with Partially Blind Signatures Based on the Discrete Logarithm Problem. *Financial Cryptography (FC'98), LNCS 1465* (pp. 296-308).

Mjolsnes, S. F. & Rong, C. (2003). On-Line E-Wallet System with Decentralized Credential Keepers. *Mobile Networks and Applications, Vol. 8, No.1*, (pp. 87-99).

Raymond, J. (2000). Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. *In H. Federrath (Ed.), Anonymity 2000, LNCS 2009*, (pp.10-29).

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method For Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of ACM, Vol.21, No.2* (pp.120-126).

Song, R. & Korba, L. (2004). How to Make E-cash with Non-repudiation and Anonymity. *In Proceedings of International Conference on Information Technology (ITCC 2004),* Las Vegas, NV, USA, April 5-7, 2004. NRC 46549.

Song, R. & Korba, L. (2003). Pay-TV System with Strong Privacy and Non-repudiation Protection. *IEEE Transactions on Consumer Electronics, Vol.49, No.2* (pp.408-413).

Song, R. & Lyu, M. R. (2001). Analysis of Privacy and Non-repudiation on Pay-TV Systems. *IEEE Transactions on Consumer Electronics, Vol.47, No.4* (pp.729-733).

Telecom Glossary 2000. (2000). Development Site for Proposed Revisions to America National Standard T1.523-2001. *Available at http://www.its.bldrdoc.gov/projects/ devglossary/t1g2k.html.*

U.S. Government. Office for Civil Rights – HIPAA: Medical Privacy - National Standards to Protect the Privacy of Personal Health Information. Available as of Feb. 28, 2005 at: http://www.hhs.gov/ocr/hipaa/

Waidner, M. & Pfitzmann, B. (1990). Loss-Tolerance for Electronic Wallets. *Proceedings of 20th International Symposium on Fault-Tolerance Computing (FTCS 20),* Newcastle upon Tyne (UK) (pp. 140-147).

Waidner, M. & Pfitzmann, B. (1991). Loss-Tolerance Electronic Wallet. *David Chaum (ed.): Smart Card 2000, Selected Papers from the Second International Smart Card 2000 Conference,* (pp. 127-150).

Yee, G. & Korba, L. (Jan. 2005). Semi-Automatic Derivation and Use of Personal Privacy Policies in E-Business. *International Journal of E-Business Research*, *Vol. 1, No. 1*, Idea Group Publishing.

Yee, G. & Korba, L. (Mar. 2005). An Agent Architecture for E-Services Privacy Policy Compliance. Proceedings, *The IEEE 19th International Conference on Advanced Information Networking and Applications (AINA 2005)*, Tamkang University, Taiwan.

[1] NRC Paper Number: NRC 48269