GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Name: Rosehaslina Razali
Practical Assignment: GSEC Version 1.3

The Overview of E-cash: Implementation and Security Issues

Abstract

There is an increase activity in research and development conducted to improve current payment system in parallel with the progress of Internet. New methodology and innovation need to be crafted to usher e-commerce to the center stage. One such innovation is the E-cash. The introduction of E-cash will brings big changes to the way businesses being conducted. E-cash will replace the conventional method of doing transaction, money become intangible item and it travels electronically across the world in more widely open network that might exposed it to all sort of risks. Therefore, the understanding of the concept, implementation issues and properties of E-cash become vital before full acceptation and implementation of the technology can take place. This paper starts by looking at the payment system historical background, follows by discussion on E-cash general concept and properties. This paper will then presents some of the E-cash implementations by some of the products vendors. A list of advantages and disadvantages of E-cash implementation is also given. Finally, this paper will conclude on the important of cryptography primitives in implementing E-cash.

1.0 History of Payment System

The oldest known trading system is barter system where goods were being exchange for the desired goods. The problem with this system was the lacking of standardization on the quantity and goods to be exchange. For example, if one has a cow and wants to trade for rice, how much rice should one received in equivalent to a cow, and if the rice's owner does not want a cow, how the trading should proceed? In solving the problem, coins and paper notes were introduced. The coins and paper notes have a market value attached to them that enable users to exchange for any desire goods and services. Using this system, one has to carry the coins and paper notes around and must has enough value in the pocket for every trading or transaction to complete.

As time progresses, the next in line is payment via checks. The checks are issued with bank agreement as a trusted body to authenticate the validity of the payers and the amount stated. This system allows consumer to make large amount of transaction without having to carry coins or paper notes around which might risk consumer to robbery. However, using this method, merchants are exposed to invalid checks where there is no money or account exists in the bank. Soon after the checks, automatic teller machine (ATM) cards were introduced to improve payment system and become the first to allow

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

transaction via electronic. ATM cards are issued by banks or by chain stores that allow consumers do shopping without a need to carry coins, paper notes or checks.

After the success of ATM cards, credit cards were introduced as a new payment scheme. The new method requires consumers to loan money from card issuers on every transaction. On each transaction, the issuers will make the payment on behalf of the consumers, the consumer then pay back the amount to the card issuers within the given period or risk being charge with interest. For both ATM and credit cards, anyone who manages to obtain the card, illegally, will be able to utilize it because there is no authentication needed upon the payment except for the signature, which also can be forged.

2.0 Introduction to E-Cash

Since the explosion of the Internet, more and more people are being hooked to the convenience Internet has to offer. Internet has connected people around the world and subsequently enables businesses to offer products and services around the globe without being physically present in front of the consumers or potential consumers. As time goes by, Internet has become apart of the daily life, which demands more and more applications being created and services being made available to make full used of the infrastructure. In line with the online business transaction, E-cash is one of the services that attract people attention for doing business transaction electronically. It is a replacement for traditional coins and paper notes, which is not viable for e-commerce. Another alternative for online payment scheme is the credit cards, however notational schemes such as credit cards require recording of transactions to be made into some individual accounts. This method requires a trust from the merchant site, which usually facilitated by verification authority such as credit-card issuer or payment gateway. Because of the "trust" requirement, this method normally eliminates user-merchant transactional anonymity. On the other hand token-based payment schemes such as E-cash does not require transactions to be recorded since the token itself allows straightforward verification by the merchant.

Even though E-cash can achieve anonymity in its implementation, it can also be implemented as traceable for higher security reason. E-cash can be implemented in two ways, on-line and off-line. On-line means E-cash is stored by the bank or issuer and consumer needs to request for it when a consumer makes payment. Different from on-line, off-line e-cash is kept by consumer in a devise such as smart card or other type of token. Each of this implementation can be classified as identified (traceable) or anonymous (untraceable). By identified implementation, it means each transaction needs verification and validation from third party such as bank. This implementation offers better security because it uses encryption and digital signature to secure and authenticate the E-cash message respectively. Identified implementation enables banks to track down individuals who actually use the E-cash to avoid double spending. This type of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

implementation is suitable for larger amount of transactions and especially for system that is available on the Internet. This method however, gives consumers less freedom compare to traditional cash transaction where consumers can spent money anywhere and anytime they want without the need of having a third party for verification.

Anonymous implementation is more close to traditional coins and paper notes payment system. The implementation is made possible by using blind/digital signature. Blind/ digital signature is used for encrypting messages and also signing for authentication purposes. When a digitally sign (blind) document is sent to a bank, the bank could ensure the authenticity of the document but does not know who sent it; therefore the consumer's identity is not revealed. The bank then signs the document making the document a certified document or in case of E-cash, the signing process produces certified E-cash. This implementation is highly suitable for micro payment. However, this type of implementation may introduce the problem of double spending and even if the banks discover the problem, it is difficult for the bank to trace the culprit who is double spending the E-cash.

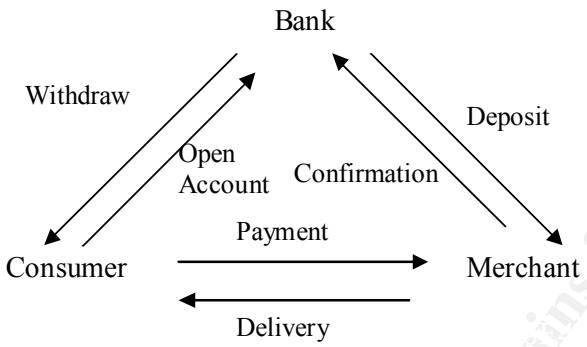
2.1 General E-Cash Implementation

So, how does E-cash work? There are many E-cash system being introduced and developed but the basic idea of E-cash is as follow. It involves at least three parties, issuer not necessarily financial institutions, consumer as the end-user who use the E-cash and merchant who accept E-cash in exchange with products or services provided.

1. Consumer needs to open an account with a bank. Merchant who wants to participate in E-cash transaction need to have accounts with various banks in order to support consumer's transaction who might use any bank account. The banks on the other hand will handle both consumers' and merchants' accounts.
2. When consumer decides to purchase, he or she will transfers the E-cash from his/her bank account to his/her electronic purse (on-line system) or E-cash token (off-line system). The E-cash can then be transferred to the merchant in exchange with the merchant's products or services. The E-cash payment can be in term of softcopy (via software) or token based. Transactions via Internet are normally encrypted.
3. Upon receiving E-cash payment from consumer, merchant will get confirmation from the bank. The bank will then authenticate the E-cash transaction. At the same time the bank will debit consumer's account based on the agreed amount. The merchant will then delivers the products or services and instructs the bank to deposit the agreed amount to the merchant's bank account.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The diagram below represent E-cash processes in general:



2.2 Properties of E-Cash

To be able to replace coins and paper notes, E-cash should be as good as coins and paper notes in term of features. Some of the important features of coins and paper notes are: transferable, acceptable, dividable, untraceable and anonymous. Listed below are some of the important properties for E-cash implementation. Later discussions on E-cash implementations will be based on these few properties.

1. Security

   For any E-cash system to be accepted, security is one of the prime concerns that need to be considered. The originality of the message being transferred among consumers, merchants and banks need to be secured to avoid any unauthorized individual intercepting or changing the content of the messages. In order to protect E-cash from such illegal activity, E-cash system must possess quality such as integrity, nonrepudiation and able to authenticate. All parties must know to whom they are dealing with, before engaging or committing in any transaction. Integrity comes in place where the message sent by consumers, merchants and banks must be intact when it reaches respective recipients. Once the integrity and authentication are achieved, consumers, merchants or banks could no longer deny the transaction.

2. Privacy

   Privacy in E-cash means the existence of anonymity for the consumers who made the payment. Similar to coins and paper notes there should not be any link or trace to individual who uses the E-cash for any transaction. This feature is needed in order to protect consumers' privacy from being monitored for the purpose of financial surveillance. However, anonymity does impose certain danger such as counterfeiting, money laundering and blackmailing. Consumers should be aware that the more anonymity offered the less security achieved by the E-cash.

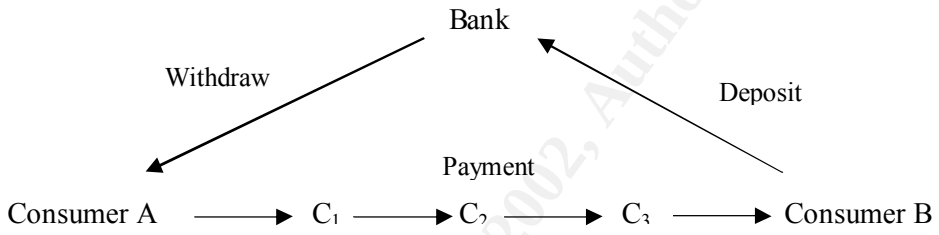
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Portability

   E-cash should be portable, similar to the conventional money where it does not depends on physical location. E-cash should be transferable via network to portable storage devices.

4. Transferability

   Transferability features allow consumers to transfer E-cash from one person to another without a need to refer to the bank. Similar to conventional cash where coins or paper notes can be transferred easily, E-cash should be able to do the same. However, this feature imposes problem where double spending could not be trace since it might have been transferred to different entities too many times. The below diagram illustrates the transferability process of E-cash.



5. Divisibility

   By divisible, it means E-cash should possess the ability to make change where E-cash can be divided into small denominations to allow small value transaction possible (this is known as micropayment). The challenge for divisible system is to be able to divide the E-cash value to small values where the total of the small E-cash value is equal to the original value. There are many systems being developed to solve divisible problem such as proposed by Eng, and Okamoto's scheme, Okamoto's scheme and Okamoto and Ohta's scheme, to name the few.

3.0 Some of The E-Cash Implementations

This section discusses some of the famous implementations of E-cash. Some companies presented might no long in operation or change name, the objective of the paper is get the understanding of E-cash implementation. The discussion will be focused on the methodology used and the properties presented earlier.

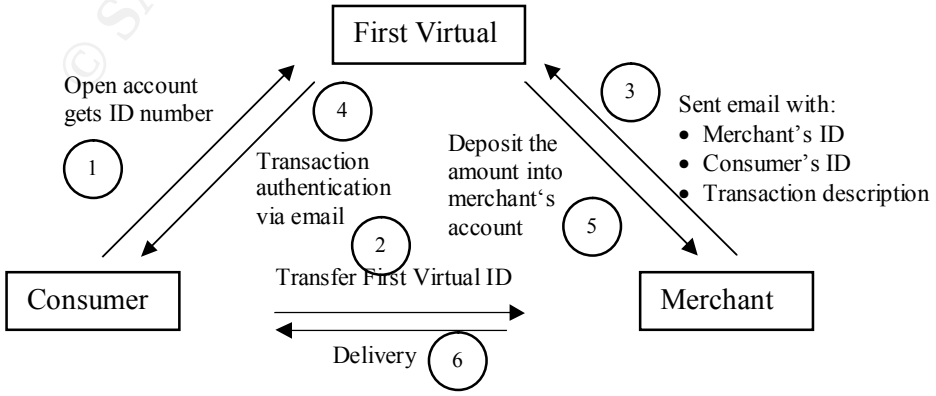
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.1 First Virtual

First Virtual Holdings founded by Lee Stein in the late 1994 is one of the first companies who offer E-cash transferable via Internet. The system depends on electronic mail as the meant of communication among consumers, merchants and First Virtual. Consumers have to give away their credit card numbers as an exchange to First Virtual E-cash. Consumers and merchants will be charge with extra charges for billing process. In summary, the First Virtual E-cash system works as follow:

1. Consumer opens account with First Virtual. Consumer must have an email account and credit card. First Virtual will give consumer an ID number as an exchange to consumer credit card number.
2. When consumer wants to purchase something from merchant who accepts First Virtual ID numbers, consumer will negotiate the price with merchant. Once agreed, consumer will give the merchant his or her First Virtual ID number.
3. The merchant then send an email to First Virtual's Internet Payment System server together with merchant's ID, consumer's IDs and description of the transaction such as the agreed price.
4. Upon receiving the merchant's email, the payment server will send an email to consumer for confirmation.
5. Consumers must reply to the email with any of these three answers:
   - YES, means consumer agrees with the transaction and allows First Virtual to instruct the bank to debit the stated amount from consumer's credit card.
   - NO, means consumer disagrees with the transaction and therefore no payment will be made. First Virtual however, will record all the refused transactions. This is done in order to avoid consumers from taking advantage of the merchants. Consumers who refuse transactions too often will then face the possibility of account termination.
   - FRAUD means consumer do not initiate the transaction. First Virtual will conduct an investigation to determine the truth.
6. Once First Virtual acknowledges that the consumer has paid the credit card company, First Virtual will credit the amount to merchant's account.

Below diagram illustrates the flow of First Virtual system.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

From the description given above, First Virtual system can be categorized as identified on-line implementation where every transaction is being recorded and traceable with the need of a third party for verification. It also means the system does not provide privacy to consumers. In addition to consumer-to-merchant transaction, First Virtual also offers person-to-person E-cash transfer; therefore the E-cash introduced is transferable. This system has shown that the used of email makes it more portable since consumers could make the transaction anytime and anywhere, as long as there is a place for accessing email. Since the Internet infrastructure is getting better by the hour, consumers should not have any problem accessing email to initiate or verify transactions.

However, this system does not use neither encryption nor digital signature when sending email from consumers-to-merchants, merchants-to-First Virtual, First Virtual-to-consumers and vice versa. Although the system claims that the security achieved by not having credit card numbers transfer on the Internet but the transfer of First Virtual ID from consumers to merchants is not secured and can be intercepted. The system also emphasize that consumers verification via email is enough to secure the transaction, but then again the email message is transfer on the open network in the plain text where the email can be intercepted and sabotaged by others. Even though First Virtual implementation does not employs encryption, it is possible for the parties involve to secured their emails and their transactions. Meaning, consumers can encrypt their emails (could use non-commercial PGP) before submitting, merchants can development secure communication applications for consumers by utilizing secure protocol such as SSL to transfer the First Virtual ID and merchants can also use secured email to send details to the banks.

3.2 CyberCash

CyberCash is an U.S.A based company, founded by Bill Melton and Daniel Lynch in 1994. CyberCash system is using what they called "Wallet" as a medium to handle credit cards, currencies, checks and CyberCoin. CyberCoin is a system to handle micropayment less than $10. CyberCash supports not only consumer-to-merchant but also consumer-to-consumer services. Below is the description of how the implementation works:

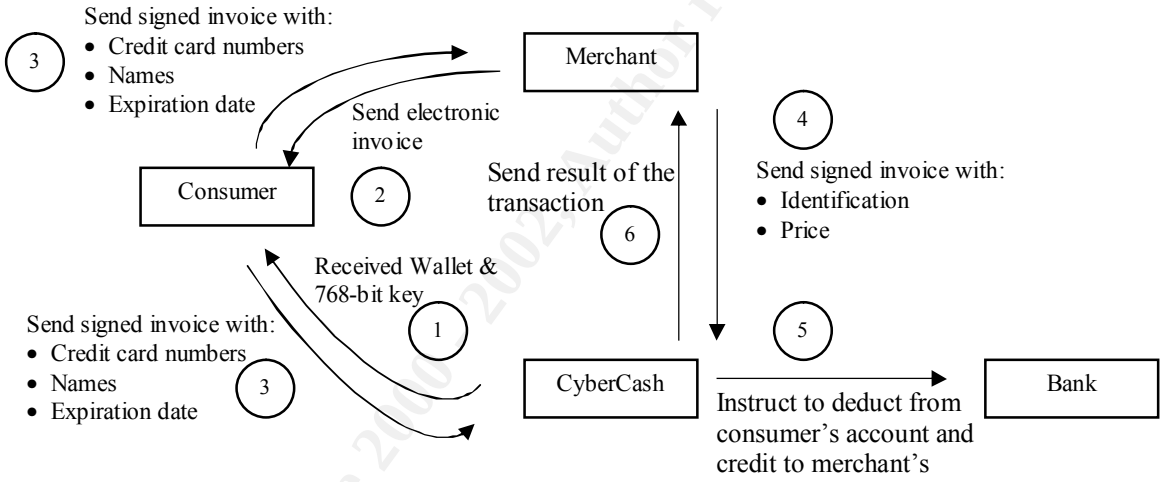
1. Consumer request "Wallet" by downloading the free software from CyberCash Internet server. The software will establish links among consumer, merchant, CyberCash and consumer's bank. Consumer then will received a 768-bit RSA key and use a password to secure the key.
2. Once consumer decides to purchase, he or she will sends his or her "Wallet" via the communication software by pressing the "PAY" button. The system will then activate merchant's CyberCash software on merchant's storefront. The merchant sends consumer an electronic invoice with the detail information of the transaction.
3. Upon receiving the invoice, consumer will sign the invoice by adding his or her credit card number, name as appeared on the card and the credit card expiration date. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"Wallet" will encrypt the signed document with CyberCash's public key and send the document to both CyberCash and merchant.

4. Merchant who received the signed document will then add merchant's identification information and price before signing it and forward it to CyberCash.
5. CyberCash who received signed documents from both consumer and merchant will unblind the document and compare the stated price. If the stated price is the same, CyberCash will instruct the bank to deduct the agree amount from consumer's credit card, credit the same amount to merchant's account. Details of the transaction are then send to the merchant.
6. Merchant will finally deliver the purchased product or service.

The below diagram summarizes CyberCash processes:



The implementation of CyberCash is based on on-line identified E-cash. Every transaction is recorded, traceable and needs third party verification. The use of encryption enables the documents to be authenticated. The system does support divisible property with the introduction of CyberCoin. However, CyberCash does not protect consumer's privacy where consumer and merchant's identities are revealed before any transaction can be completed. In term of portability, "Wallet" can only be installed on consumer's computer; therefore consumer could only make transactions from a computer where the "Wallet" is installed. This system support both transfers but from consumer-to-consumer and consumer-to-merchant transfers.

3.3 DigiCash

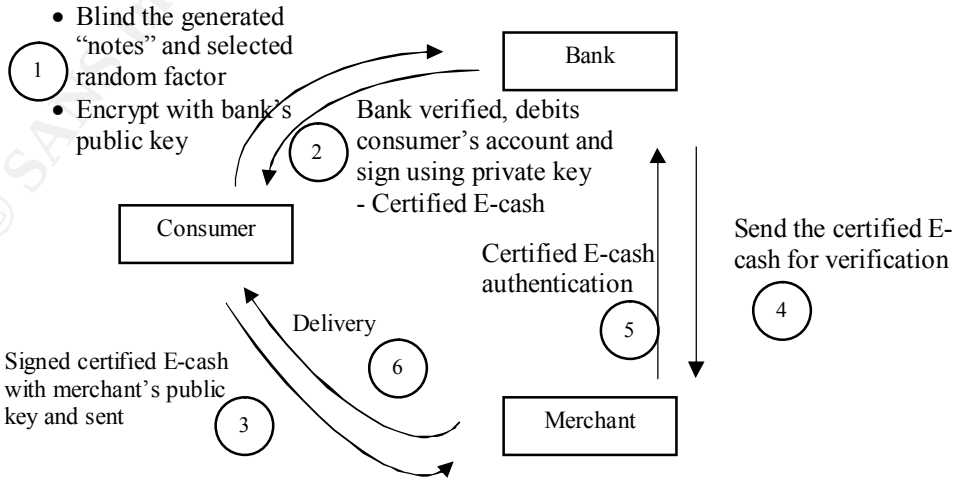
Founded by David Chaum in 1994, Digicash is located in Amsterdam. The system was designed based on Chaum's digital cash system. DigiCash system uses digital signature for encryption and "blind" signature for authentication to ensure the security of transactions and to protect consumers, merchants and banks from illegal activities.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DigiCash was designed to provide payment from one computer to another computer through Internet. DigiCash offers both anonymity and identified for both of its on-line and off-line services. The E-cash product introduced by DigiCash is called "ecash" where it uses RSA encryption algorithm. The system works as follow:

1. Consumer who wants to use DigiCash must open an account with bank that provides on-line DigiCash system.
2. Ecash software will generate a pair of keys, private and public keys when it is first executed on consumer's computer. The consumer will keep the private key, which is use to sign E-cash transactions originated from consumer. Public key will be made available for banks, merchants and other people to verify any messages or E-cash transferred from consumer.
3. When consumer decides to purchase, consumer's computer will determine the denominations based on the amount needed and generate matching random serial numbers acting as "notes" for each denomination. The consumer's computer will also generate a selected random factor use to blind the denominations/random serial numbers. The blinded random serial numbers or the blinded "notes" are then encrypted with the bank's public key before sending it to bank for certifying.
4. The bank decrypts the message using it's private key. Once the message is decrypted, the bank will debit the amount found from the message from consumer's account. In exchange with the debited amount, the bank then certified the blinded "notes" found in the message with it's private key. The signed blinded "notes" is then send back to consumer who will take out the blinding factor before using the "notes" in payment. Both the random serial numbers (the "notes") and the signatures (consumer's and bank's) are the certified E-cash.
5. Upon payment, the certified E-cash is sent to merchant who will send it to the bank for verification. The bank will verify whether E-cash is valid and have not been used before.

The diagram shown below is the visualization of the above process:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DigiCash system offers both anonymity for on-line and off-line services and the system allows transfers from consumer-to-consumer in additional to consumer-to-merchant. The certified E-cash is portable since it is a softcopy based, where it can be stored and transferred to other devices, making it easy and convenient to use. It also protects consumer's privacy via blind signature. The bank cannot make any connection as to who signed the document because only consumer know the random factor use in the blind signature. Another property is the divisible feature that comes from the introduction of CyberCoin to handle micropayment. In term of security, DigiCash provides better security by using digital signature to authenticate the message send and received. Using this approach, bank's public key is available for both consumer and merchant, making it possible for both parties to authenticate the message. However, both parties are unable to forge bank's signature since only the bank has the matching private key to sign (certified) the E-cash. Consumer is also being protected against illegal merchant activities and mistreated attempts by bank.

3.4 Mondex

The development of Mondex started in the early 1990s. The concern on security has brought Mondex (E-cash application) and Multos (E-cash smart card based operating system) to the highest achievement in security recognition; level E6 was awarded in 1999 by UK IT security Evaluation and Certification (ITSEC). Recognition has proved that Mondex is one of the most secured E-cash applications available today. Mondex is an E-cash application, based on smart card where the E-cash is stored in the chip located in the smart card.

The concept of Mondex is similar to DigiCash. Consumer requests E-cash from bank. When consumer decides to purchase, consumer's E-cash will be transferred to the merchant who will then send it to the bank for verification and cashing. Upon receiving the E-cash, bank will verify and certify the E-cash, at the same time consumer's accounts will be debited and the same amount will be credited to the merchant's account. Finally, the merchant will deliver the products or services to the consumer. Mondex is offering anonymity on both of its on-line and off-line services. For off-line transactions, merchant can do verification after the transaction completed (This might expose merchant to double spending that is difficult to trace). Besides consumer-to-merchant transaction, Mondex also allows consumer-to-consumer E-cash transfer. In short Mondex had full-filled almost all the desirable properties of E-cash mentioned earlier. It has security, which is based on digital signature where each message transfer among bank, merchant and consumer can be authenticated. The system is portable with the use of smart card. Mondex system also protects consumer's privacy by using blind signature. In term of divisibility, Mondex declares that the system is able to handle micropayment as small as one cent.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4.0 Advantages of E-Cash

To consumer, E-cash is more than a convenient way of carrying cash, since it also opens avenue for e-commerce to take place. Consumer only needs to have smart card like devices to initiate transaction, either on-line or off-line. For some implementations, E-cash can be stored in a computer for easy transfer over the Internet for on-line transaction. Anonymity implementation gives consumer a privacy to use E-cash just like the conventional coins and paper notes. Consumers are also able to make transactions without the need of third party verification. E-cash environment enables consumers to purchase small item over the Internet, which is cumbersome in other implementations such as credit cards. To merchant, E-cash provides an opportunity to expand their businesses across the globe without the barrier of different currencies. By using identified approach, merchant can be protected against fraud, since each transaction needs verification from financial institutions or banks. For the banks, E-cash implementation does reduce cost in maintaining cash in the bank and therefore increase bank management efficiency. Furthermore with E-cash, banks are now able to provide their services to the world via the Internet more easily.

5.0 Disadvantages of E-Cash

One of the disadvantages of E-cash is the existence of counterfeiters who are able to recreate E-cash either stored in smart card or softcopy based. All parties involve, consumers, merchants and banks/issuers, are affected by this counterfeit activity. Liability of the loss E-cash on damage smart card or crashed computer where the E-cash is installed is also in question. Although the number of Internet users is increasing in number, there are many others who do not have the opportunity to own computers and get connected to the Internet. These are the people who will be left behind even further with the introduction of the E-cash. Not to mention that consumer needs to learn new things such as installing software on the computer and understand how E-cash software operates. Furthermore, the numbers of participating companies are still low and it seems companies are not willing to accept e-cash system in order to attract more consumers. This phenomena might relate to the fact that additional fee is incur as processing charges by banks to merchant and consumer. These additional charges are non-issue in conventional payment system but can mounting to a huge sum in E-cash implementation. Other issue of E-cash is money monitoring by the government. With the conventional coins and paper notes, government can monitor money flow to stabilized economy, but with E-cash, there is no foreseeable way for the government to control the flow of E-cash in and out of a country. Even more mind-boggling is how a government can calculates or collects taxation from untraceable E-cash asset.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

6.0 Conclusion

The discussion above shows that cryptography primitives such as encryption, digital signature and blind digital signature play an important role in implementing E-cash. Encryption enables all entities, consumers, merchants and banks to verify the originality of the message received. The result of digital signature, certified E-cash, established a strong trust between merchants and consumers. Therefore, any illegal activity such as forgery by consumers or merchants can be avoided because only trusted entities such as banks or issuers are able to authenticate the certified E-cash. The introduction of blind signature concept that is similar to digital signature (except the identity of the consumer being leave out), gives consumers the freedom and privacy (anonymity) to spend their E-cash without being monitored. In addition, consumers have the choice to use either blind signature or digital signature to ensure security level of the transaction made, especially when it involves macropayment. Finally, the highest recognition ever received in security field by Mondex (Level E6 by ITSEC) has shown the dedication work towards establishing security to ensure E-cash implementation becomes a reality and accepted by all. The award also indicates the possibility of E-cash to become the next payment system for the future.

7.0 References

[1] A. Kirch, C. Anderson, C. Butler, D. McMahon, L. Parks, and R. Murtha, "Exploring Digital Cash," *Available from URL: http://www.sims.berkeley.edu/courses/is204/f97/GroupE/onepage.html*

[2] CyberCash homepage, *Available from URL: http://www.cybercash.com/*

[3] D. Chaum, "Achieving Electronic Privacy," *Available from URL: http://ntrg.cs.tcd.ie/mepeirce/Project/Chaum/sciam.html*

[4] D. G. Post, "E-Cash: Can't Live With It, Can't Live Without It." *Available from URL: http://www.cli.org/Dpost/X0008_ECASH.html*

[5] D. McCullaqh, "Digging Those Digicash Blues," Available from URL: *http://www.wired.com/news/ebiz/0,1272,44507,00.html*

[6] F. Stalder, "Digicash: Learning from Failure," *Available from URL: http://www.heise.de/tp/english/inhalt/te/1643/1.html*

[7] J. Miller, "E-money mini-FAQ (release 2.0): Answers to Frequently Asked Questions about Electronic Money, or E-money, and Digital Cash", *Available from URL: http://www.ex.ac.uk/~Rdavies/arian/emoneyfaq.html*

[8] M. Cipparone, "Digicash Convertibilities – A Look Into The Future," *Available from URL: http://www.arraydev.com/commerce/JIBC/9601-5.html*

[9] M. J. Farsi, "Digital Cash," *Available from URL: http://www.simovits.com/archive/dcash.pdf*

[10] Mondex homepage, *Available from URL: http://www.mondex.com/*

[11] T. Eng and T. Okamoto, "Single Term Divisible Electronic Coins, Advances in Cryptology EUROCRYPT '94" *Springer-Verlag, pp. 311-323.*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[12] T. L. Chien, "Electronic Cash: Current Status and Outlook," *Available from URL: http://misdb.bpa.arizon.edu/~alivia/class/mis581/StudentWork/Chienting/cash.html*

[13] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme, Advances in Cryptology CRYPTO '95," *Springer-Verlag, pp. 438-451.*

[14] T. Okamoto, and K. Ohta, "Universal Electronic Cash, Advances in Cryptology '91," *Springer-Verlag, pp. 324-337.*

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.