The Secure Electronic Check

Final Term Paper

Team Members:

2001134 Choi, MiJin
2001046 Park, JungHo
2001019 Kim, MinJi
2001111 Jun, WooSuK
INDEX

1. Introduction
2. Backgrounds
   2.1 Electronic Check Flow
   2.2 Secure Electronic Check
   2.3 Electronic checkbooks
   2.4 Fraud Prevention
3. Proposed Secure Electronic Check
   3.1 Current Problems of E-check System
      3.1.1 Invalid account
      3.1.2 NSF (Not Sufficient Fund).
   3.2 Software Based Checkbook System
   3.3 Smartcard Based Checkbook System

4. Payer and Payee Systems
   4.1 Payer System
      4.1.1 Network Interface
      4.1.2 Incoming Invoice Processing
      4.1.3 Payee Directory
      4.1.4 Accounts Payable Interface
      4.1.5 User Interface
      4.1.6 Check Writing
      4.1.7 Check Register
   4.2 Payee System
      4.2.1 Check and Attachment Verification

5. Checkbook Distribution and the Public key Infrastructure

6. Other Systems
   6.1 NetBill
   6.2 NetCheque

7. Conclusion
8. References
The Secure Electronic Check

1 Introduction
The Electronic Check was developed by a project of the Financial Services Technology Consortium. The FSTC is comprised of about 100 members, including most of the major banks, suppliers of technology to the financial industry, universities and research laboratories. The technical work of the Electronic Check Project was carried out in a number of phases: generating the original concepts, performing preliminary research, building and demonstrating a prototype, formulating specifications for a pilot system, and implementing the pilot system.

The electronic check is designed to perform the payment and other financial functions of paper checks, by using cryptographic signatures and secure messaging over the Internet. The electronic check system is designed with message integrity, authentication and non-repudiation properties sufficient to prevent fraud against the banks and their customers. It is compatible with either interactive web transactions or with electronic mail. Since the electronic check does not depend on real-time interactions or on third party authorizations, electronic checks are better able to survive outages of network links and computing nodes. The result is a highly efficient electronic payments system, with a technology base that is extensible to a variety of financial instruments and other high-integrity document processing applications needed by the financial industry.

Based on standard electronic check, we suggest a more secure transaction in the B2B and B2C. And then we will briefly look around electronic check under development.

2 Backgrounds
2.1 Electronic Check Flow
In the example shown in Figure 1, the business transaction begins with the payee sending an invoice or bill to the payer, which is processed by the payer’s accounts payable system. When the time comes to pay the invoice, the invoice information is retrieved from the accounts payable system, and the invoice data is used to create an E-check. The E-check includes familiar check information such as the payee’s name, the amount, and the date and the account information. To sign the E-check, the payer enters a PIN to unlock an electronic checkbook card in the form of a smart card. This card is a secure container for the payer’s private signature key, and assures a degree of non-repudiation. The signature on the E-check may also cryptographically bind a copy of the invoice to the E-check, so that an attacker cannot substitute a different invoice in order to commit fraud. The invoice format is not fixed, but it can be flexible with respect to length, format and data content, so that the payer can return the document received from the payee. This provides the payee with the complete information
E-checks have been designed so that the integrity, authentication and non-repudiation properties of the transaction, since the entire contents of the E-check are machine-readable. Finally, the payer receives a line item on his statement, which may now carry a full description of the transaction, since the entire contents of the E-check are machine-readable.

Figure 1. Basic Electronic Check Flow

The signed E-check and invoice is sent to the payee by email or a web transaction. The payee verifies the payer's signature on the E-check and invoice, detaches the invoice information, and posts the payment to accounts receivable. The payee enters his PIN to unlock his electronic checkbook and uses the electronic checkbook to endorse the E-check and to sign an electronic deposit slip to deposit a batch of E-checks.

The endorsed E-check is forwarded to the payee’s bank for deposit and subsequent clearing. The clearing process can be done by integrating E-check into existing Electronic Check Presentment systems or other clearing and settlement systems. Both the payee’s bank and payer’s bank verify all signatures on the E-check and endorsement using a two layer certificate system which links the signature verification keys to the signer and signer's bank account. The paying bank verifies that this transmission of the E-check is not a duplicate, that the payer's certificate and account are currently valid, and posts the E-check to the payer's Demand Deposit Account.

Finally, the payer receives a line item on his statement, which may now carry a full description of the transaction, since the entire contents of the E-check are machine-readable.

E-checks have been designed so that the integrity, authentication and non-repudiation properties of
public key signatures are sufficient to protect against fraud. Furthermore, to protect the paper check accounts against fraud, E-checks use different bank account numbers, which are valid only for cryptographically signed E-checks. Since encryption is not required to prevent fraud, the E-check technology is compatible with export policies regarding encryption technology. The E-check may be encrypted over any of the transmission links for privacy reasons, using encryption technology of a type and strength consistent with regulations governing each situation. Furthermore, the payer and payee are not anonymous to their respective banks, and E-checks are compatible with legal requirements to report certain types of financial transactions.

2.2 Secure Electronic Check

The E-check flow shown in Figure 1 is typical, but E-checks can be used in other ways, just like paper checks.

Figure 2 shows a certified electronic check flow. In this case, the payer sends the E-check to the payer's bank. The payer's bank verifies the payer's signature, determines that there are funds available in the payer's account, and places a hold on the funds. The payer's bank then countersigns the check to certify it, and send the check back to the payer. Alternatively, the bank can send the certified check directly to the payee, possibly over an encrypted channel to provide the payee with the greatest degree of security and confidentiality.

2.3 Electronic Checkbooks

A handwritten signature captures the reflexive movement of the signer's muscles and is partly a
biometric characteristic of the signer. This makes it difficult for a forger to create a perfect forgery, even if the forger has a sample of a handwritten signature. However, a perfect forgery of a cryptographic signature can be made by anyone who has the signer's private signature key. Therefore, it is critical to establishing an E-check system based on public key signatures that payees and banks are able to trust that payers can maintain possession and control over their private signing keys at all times. Electronic checkbook smart cards or other cryptographic hardware are used to help ensure that signatures are made only by legitimate signers, so that check forgery is made difficult. Electronic checkbook cards also standardize and simplify key generation, distribution and use, so that a high and uniform level of trust can be established without depending on the skill and diligence of every E-check customer.

2.4 Fraud Prevention

A design goal of the E-check system is to prevent fraud without relying on encryption, since standard widespread availability of strong encryption has been hampered by export controls and by attempts to regulate its use. Cryptographic signature systems are quite freely used and exported, while key management and public key infrastructure components are more restricted, especially if they can also be used to manage encryption keys.

Features intended to prevent fraud include:

1. Duplicate detection: Each E-check is guaranteed to be unique by the operation of the electronic checkbook. The payee and payee's bank should detect and refuse duplicate submissions of E-checks, and the payer's bank must detect duplicates and pay only one instance of an E-check. This prevents multiple payments due to innocent retransmissions of email, and also prevents a payee from cashing and depositing an E-check in two different accounts.

2. Payee identification: The check block provides for checks to be made out to the payee's bank routing code and either an account or customer ID number. It also provides for an E-check to be made out to the payee's public key. These parameters uniquely identify the payee, and prevent an eavesdropper from exploiting the ambiguity of payee identification which otherwise exists if only payee common names are used. These parameters are also included in the endorsement block so that E-checks can be endorsed over to uniquely identified third parties.

3. Electronic account numbers: The account number in the account block is a randomly chosen number assigned by the bank for the purpose of writing and depositing E-checks. The payer's and depositor's E-check account numbers are mapped to their paper check account numbers by their respective banks. The banks will not accept paper checks or drafts written against the E-check account numbers. This prevents an eavesdropper or corrupt payee from printing and passing paper checks or drafts against the account numbers.
4. Cryptographically attached invoices: Invoice and attachment blocks can be sent with the E-check blocks to detail the purpose of the payment. These blocks can be signed by the E-check signature, which binds these documents to the E-check and ensures their authenticity and integrity. This prevents an attacker from, for example, intercepting an E-check and purchase order, changing the delivery address in the order, and forwarding the E-check and altered order to the merchant.

3 Proposed Secure Electronic Check

Main Problems in current E-check system.

Check is payer-centered payment system. Therefore, there are several problems in current offline and online E-check system when payee receives checks.

3.1 Current Problems of E-check System

3.1.1 Invalid account.
Check is supposed to be received anywhere. However, payee can not trust payer if payee doesn’ t have any transactions before. Even though payee has had some transactions before, how can payee trusts if payer still has his or her account at the bank?

3.1.2 NSF (Not Sufficient Fund).
Let’ s assume that payee trust payer has valid account, but can payee trust payer has enough money in the bank account? Payer usually deposits enough money not to go into bankruptcy. However, if payer has malicious purpose and go into bankruptcy, then who’ s going to be damaged? Payee will be damaged totally. Therefore, payee can not receive a suspicious check. Then is that possible to distinguish fine checks from malicious checks? No. Never. That force payee not to receive checks and finally whole system will be failure. In cyber space that problem will be more serious.

Above topics are nowadays hot issues in the E-check system development. Especially first issue has been researched in many ways, so we focus on the NSF problem in software based checkbook and smartcard based checkbook system.

3.2 Software Based Checkbook System
This system is based on credit information system already existing.
Payer can use certain value of checks according to payer’ s credit granted by payer’ s bank. If payer want to buy more expensive thing than payee may buy according to the credit, payee can ask payer to get certification from the bank. Payer sends Echeck to bank to get certification. When bank
certify the E-check, bank check the payer’s account and reserve certain percentage of balance according to the invoice issued by payee and returns the certified E-check. Through this procedure payee can reduce the possibilities of bounce. Also payer can use E-check much more stores.

### 3.3 Smartcard Based Checkbook System

![Figure 3. Smartcard Based Checkbook System](image)

E-check is also used with smartcard in the offline environment. In this case payer can’t get certification from the bank by himself. Smartcard has payer’s credit information and payee can check the level of credit. Therefore, payer can pay based on the credit information in the card. However, payee has the same problems that how payee can trust payer has enough money when payer pays.

Payee asks payer to get verification using payee’s terminals at the store. Using smartcard payer connects the bank and asks verification. Bank will do the same procedure of software based checkbook system.

At this time, there is no definition of the electronic checkbook interface at the smart card connector. When electronic checkbooks are used at point of sale terminals, then a connector level interface will need to be defined, including all protocol levels from electrical signals up to the application level.

A smart card may not be the best device for use at point of sale terminals. Alternatives may include electronic checkbook functionality built into PDAs (Personal Digital Assistants) such as the 3COM Palm III. In this case, infrared links may be used instead of electrical
contacts. Use of a PDA for check writing may have security advantages over smart cards, since the user has an independent display and data entry capability, and the user does not have to trust the merchant terminal.

4 Payer and Payee Systems

Payer and payee systems are used to write E-checks, verify signatures, endorse E-checks and prepare deposits for transmission to the banks. They also provide network interfaces and may provide interfaces with directories. They may also automate the process of E-check attachments such as invoices, remittance information and advice of payment documents, and they may provide mechanized interfaces to the user's accounting systems. The design of these systems will depend on the types of network services used, the degree of desired automation, the legacy accounting systems, and the design approach of the payer and payee system vendor. The functional diagrams in the following sections are intended to describe typical functions that must be carried out, but they do not dictate actual designs.

4.1 Payer System

Figure 4 shows a functional diagram of a payer system.

4.1.1 Network Interface

At the right side of Figure 4 is the network interface. This may be based on an email client, an email server or an SSL/HTTP client. Functions provided in the interface for a mail client system would include:

- Firewall functions or other functions to protect the payee's operating system from penetration
- POP3 (Post Office Protocol) mail client
- S/MIME (Secure-Multipurpose Internet Mail Extensions) decryption of incoming mail and encryption of outgoing mail
- Mail logging or archiving.
4.1.2 Incoming Invoice Processing

Processing of incoming invoices is especially important for the case of commercial payments using E-checks. A significant benefit of using E-checks for payment is the ability to receive invoices and return them with the payment so that the payee knows how to accurately post the payments in accounts payable.

Information about the payee can be extracted and stored in the payee directory, and the invoice itself is passed to accounts payable until the payment is approved and due.

4.1.3 Payee Directory

The payee directory includes payee email addresses, payee encryption keys and certificates, and the payees' E-check certificates and account blocks if the payer wishes to write checks payable to the payee's account or key in order to uniquely identify the payee. These may have been received in an invoice or in a payment previously received from the payee.

4.1.4 Accounts Payable Interface

The design of the interface to accounts payable will depend on the payee's accounts payable system. These may vary from a paper interface, or comma delimited text files, to more sophisticated file transfers, database interfaces or APIs. When a payment is due it is initiated by information received from accounts payable.
4.1.5 User Interface

Functions provided via the user interface include:
- Approval of payments initiated from accounts payable
- Manual initiation of check payments or corrections
- Entry of PINs to unlock the check signing and administration features of the electronic checkbook
- Review of the check register and initiation of any reports or audits based on its contents and administration of the payee system.

4.1.6 Check Writing

Functions provided by check writing include:
- Receiving information needed for the check such as payee, date, and amount
- Formatting the information into an FSML document ready to be signed by the electronic checkbook
- Appending the payee's certificates, account blocks, and any attachments or invoice blocks
- Unlocking the electronic checkbook using the PIN received from the user
- Interacting with the electronic checkbook to sign the E-check
- Updating the check register
- Passing the signed E-check and attachments to the mail system along with payee directory information

4.1.7 Check Register

The check register contains a record of E-checks written by the payee. It should be compared periodically with the secure log/register contained in the electronic checkbook.

4.2 Payee System

Figure 5 shows a functional diagram of a payer system. Many of the functions are the same as for the payer system, and in practice bank customers would have systems that include all functions needed to write, endorse and deposit E-checks.
4.2.1 Check and Attachment Verification

After the incoming E-check and attachments have been received and optionally decrypted by the network interface the check and attachment verification function performs the following functions:

- Receives an email and determines that it contains an E-check
- Parses the FSML
- Cryptographically verifies the signatures on the E-check, the account block, and certificates from a trusted root public key
- Evaluates the pay-to, date, account restrictions and other data contained in the E-check to determine that the E-check is properly formed, valid and intended for the payee
- Determines whether the E-check is a duplicate of one received in a previous transmission
- Displays any failures or errors to the user interface
- Detaches any attachments or invoices returned by the payer as an advice of payment
- Makes the E-check available for endorsement and deposit

It should be noted that E-checks can be verified without use of the electronic checkbook hardware.
4.2.2 Endorsement and Deposit Processing

Endorsement and deposit processing does require the use of the electronic checkbook. The functions performed include:

- Receiving information needed for the endorsement and deposit blocks
- Formatting the information into an FSML document ready to be signed by the electronic checkbook
- Appending the payee's certificates, account blocks, and any attachments or invoice blocks
- Unlocking the electronic checkbook using the PIN received from the user
- Interacting with the electronic checkbook to endorse each check
- Interacting with the electronic checkbook to sign the deposit
- Updating the check register
- Passing the endorsed checks and deposit to the mail system for transmission to the payee's bank.

5. Checkbook Distribution and the Public Key Infrastructure

Electronic checkbook distribution can vary considerably among banks so long as basic requirements are met. These include:

- Bank signed X.509 certificates and account blocks meet FSML specifications
- Electronic check hardware, firmware and software meet the electronic checkbook requirements and API specifications
- Bank certificate authority policies meet regulatory and legal requirements

A typical approach to electronic checkbook distribution is shown in Figure 6. Some of the operations shown, such as card initialization and the bank certification authority, may be carried out by other firms, acting as agents of the bank.
The steps in the process are as follows:

1. Marketing and sales contacts a customer who is interested in electronic checking.
2. The customer signs up for electronic checking, either by adding to an existing account or by opening a new account. The information collected from the customer includes the usual customer name, address, telephone, etc, as well as information about the PC or server hardware, operating system and email account that the customer will be using for electronic checking.
3. The information is entered in the bank administrative systems used to manage opening of new accounts.
4. Electronic checkbook issuance instructions are sent to the card initialization operation. Data includes all the information needed to initialize the signer personal data, the account block, and the X.509 certificate for the account. This requires that the bank administrative systems have assigned the electronic account number. Other information may be included to initialize use of the electronic checkbook card as a cash card, debit card or charge card.
5. The card initialization operation generates a key pair in the card, extracts the public key, and sends the account block and X.509 certificate information to the bank certification authority for signing.
6. The certification authority signs the X.509 certificate and the account block using the bank CA's private signing key, and returns the certificate and account blocks to card initialization.
7. The bank CA also sends the certificate and account block to the bank E-check server to update its data base with the pending account.
8. The certificates and account blocks are installed in the card, the card is printed, and the PINs are initialized. A PIN mailer is printed and sent to the customer. The card may be embossed, and the
magnetic stripe may be written to enable other card functions.

9. The electronic checkbook, smart card reader, software and instructions are assembled in a kit and shipped separately to the customer.

10. Card initialization notifies the account administrative systems that the card has been sent.

11. The account administrative systems activate the account in the bank E-check server, possibly after receiving an email or other confirmation from the customer.

12. If the card is lost or stolen, the customer reports it to the bank. The bank CA revokes the certificate and notifies the bank server of the revocation. Other banks may be notified by CRL, and the bank may take other actions with respect to the account.

6. Other Systems
There are some cases under development in USA. NetBill is designed by Carnegie Mellon University and Netcheque is developed at the Information Sciences Institute of the University of Southern California. A brief description of the system is followed below.

NetBill
The NetBill Project is developing standard interfaces for interactions among a consumer's client, a merchant's server, the NetBill system, and existing banking and credit institutions. These interfaces, implemented in portable software modules, can be linked to independently developed client or server software that runs on multiple platforms and supports diverse network-based services - each of which can use NetBill services provided by one or more financial services organizations. NetBill also uses Kerberos tickets. The NetBill transaction protocol involves several phases, for price negotiation, goods delivery, and payment; only the last of these phases requires non-repudiable signatures. Instead of using public key cryptography for message authentication and encryption throughout the NetBill system, we use symmetric cryptography because it offers significant performance advantages.

1. Netcheque
The NetCheque system is a distributed payment system based on the credit-debit model. The strengths of the NetCheque system are its security, reliability, scalability, and efficiency. Signatures on checks are authenticated using Kerberos. Reliability and scalability are provided by using multiple accounting servers. NetCheque is well suited for clearing micro payments; its use of conventional cryptography makes it more efficient than systems based on public key cryptography. Though Netcheque does not itself provide anonymity, it may be used to facilitate the flow of funds between other services that do provide anonymity. The principal weakness of NetCheque at this time is its small initial customer base. Users of Netcheque must be registered as Netcheque users before
they can make payments. However, once registered with one server, checks written by the user may be cleared through any NetCheque server.

7. Conclusion
Electronic check system is designed for the substitution of paper based check system in U.S. However, for the characteristics of the system, E check system has the opportunity that it can be used in B2B transactions and in the micro payment of B2C transaction. Due to nonexistence of actual E check system proposed by FTSC which is on the run in commercial, though we could not find out the exact problems which can be occurred on the implementations and operations. We could find out the problems that the merchants can be damaged, during the transactions like B2B or macro payment, for it imitates the original electronic check which runs offline. Therefore we tried to think and find out the way to overcome these problems and to apply the electronic check system to domestic B2B or B2C transactions.

8. References
2. http://www.ini.cmu.edu/netbill/
5. Çѱ¹ÀÇÀüÀÚ»ó°Å·¡ȯ°æÀ»°í·ÁÇÑÀüÀÚÁöºÒ½Ã½ºÅÛÀÇ¼º°ø¿äÀÎºÐ¼®ÁÖÀçÈÆ, °æ¿µÁ¤º¸Çبּ¸Á¦9±ÇÁ¦1È£Çѱ¹°æ¿µÁ¤º¸ÇÐȸ. 1999. 3. 77-98
8. http://www.w3.org/pub/WWW/Payments/