ELECTRONIC CHEQUES

Recent years have seen a tremendous increase in e-commerce transactions. The success of e-commerce relies on developing adequate payment technologies. One such technology is e-cheque. An e-cheque is an electronic document which substitutes the paper check for online transactions. Digital signatures (based on public key cryptography) replace handwritten signatures. The e-cheque system is designed with message integrity, authentication and non-repudiation features, strong enough to prevent fraud against the banks and their customers. The minimum security requirements supported by the e-cheque system are as follows :

Confidentiality : keeping information (e.g. e-mail message, payment order,etc) secret.

Authentication : knowing and verifying the origin and/or destination of information.

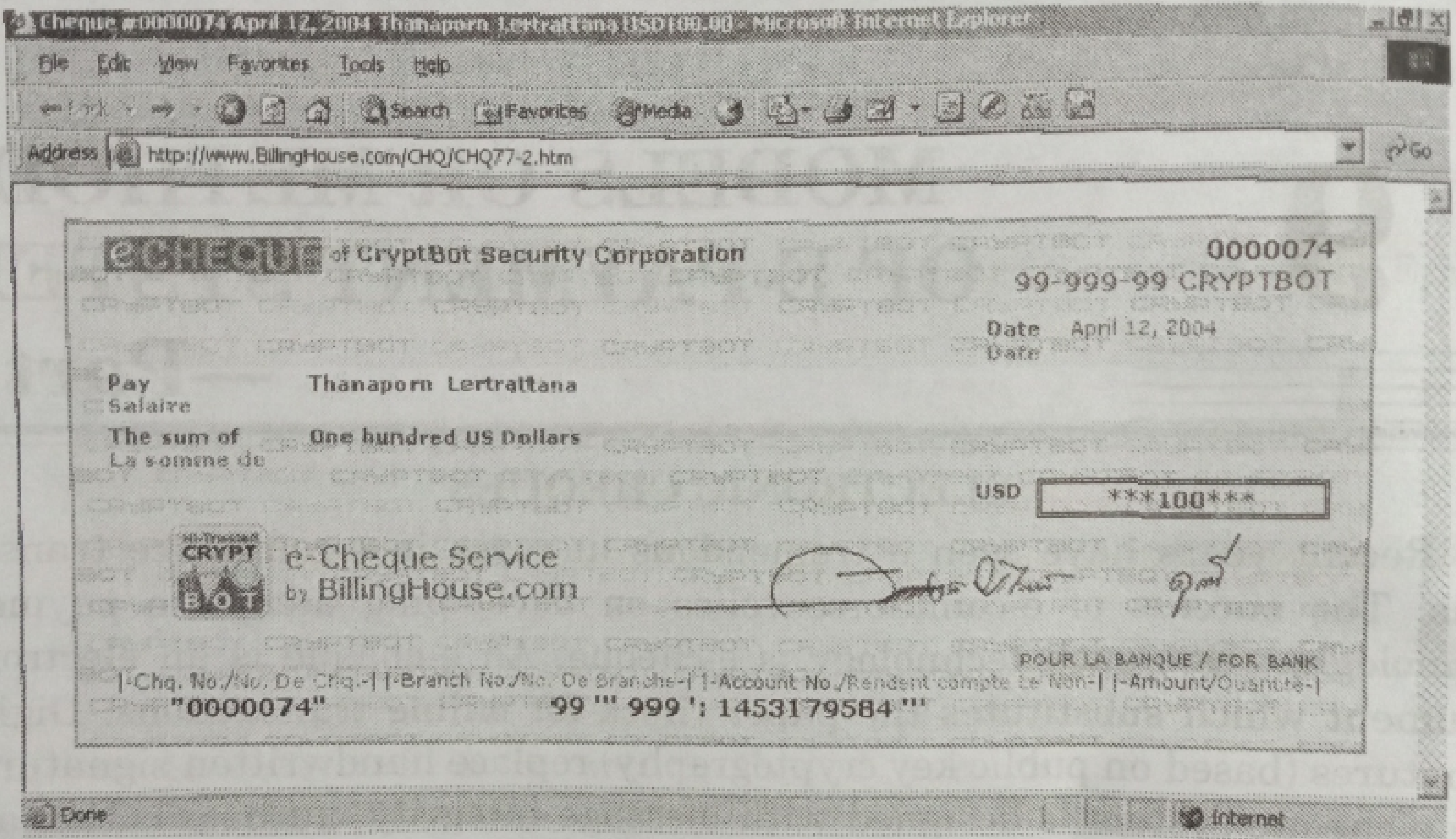
Integrity : verifying that the data hasn't been tampered with.

Non-repudiation : knowing that the data, once sent cannot be retracted ordenied. The e-cheque is compatible with interactive web transactions or with email and does not depend on real-time interactions or on third party authorizations. It is designed to work with paper cheque practices and systems, with minimum impact on payers, payees, banks and the financial system.

Payers and payees can be individuals, businesses, or financial institutions such as banks. e-cheques are transferred directly from the payer to the payee, so that the timing and the purpose of the payment are clear to the payee. The payer writes an e-cheque by structuring an electronic document with the information legally required to be in a cheque and digitally signs it. The payee receives the e-cheque over email or web, verifies the payer's digital signature, writes out a deposit and digitally signs it.

The payee's bank verifies the payer's and payee's digital signatures, and then forwards the cheque for clearing and settlement. The payer's bank verifies the payer's digital signature and debits the payer's account. Like paper cheques, e-cheques can bounce or be returned, for stop payment instructions, insufficient funds or accounts being closed

The electronic cheques are modeled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the Internet...



Cheque #0000074 April 12, 2004 Thanaporn Lertrattana USD100.00 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Done
Internet

http://www.BillingHouse.com/CHQ/CHQ77-2.htm

eCHEQUE of CryptBot Security Corporation

0000074
99-999-99 CRYPTBOT

Date April 12, 2004
Date

Pay Thanaporn Lertrattana
Salaire

The sum of One hundred US Dollars
La somme de

USD ***100***

CRYPT BOT e-Cheque Service
by BillingHouse.com

POUR LA BANQUE / FOR BANK

|-Chq. No./No. De Chq.-| |-Branch No./No. De Branche-| |-Account No./Rendent compte Le Non-| |-Amount/Quantite-|

"0000074" 99 ''' 999 '; 1453179584 '''

Figure 9.1 : Shows digitally signed e-cheque

Electronic cheque is messages that contain all the information that is found on an ordinary Cheque but in this cheque digital signature use for signing online documents and support.It has digital certificate to authenticate bank account. So many websites uses Electronic Cheque. An electronic cheque is another form paper cheque but this cheque fulfill the demand of security of consumer transaction and offers many more features for further processing .Electronic checks are typically used in orders processed online and are governed by the same laws that apply to paper checks. Electronic checks offer protective measures such as aunthentification and digital signatures to safeguard digital transactions.

THE E-CHEQUE PROTOCOLS

The majority of e-payment systems on the Internet today are based on three-party communication protocols involving a trusted third-party besides the payer and payee. The trusted third-party is neededto authenticate and verify the payment or the transaction process between the clients. Unfortunately this decreases the system performance because of the increased number of messages that must be exchanged. The e-cheque system has been optimized so as to work with only two parties, namely the payee and payer. The e-cheque operational scenarios are structured around five main protocols as follows :

1. System Setup.
2. Client Registration.
3. Cheque Withdrawal.
4. Cheque Payment.
5. Cheque Deposit.

System Setup : Each client that wishes to use the e-cheque system must obtain a digital identity. A digital identity is achieved by obtaining a valid digital certificate from a recognized certificate authority (CA) (e.g. Verisign). The working scenario for obtaining a digital identity is as follows :

1. An asymmetric key pair (private/public key) is generated on the client side.
2. A certificate request (CRQ) is compiled including both information about the requesting subject (purpose of the requested certificate) and the public key.
3. The CRQ is signed using the newly generated private key.
4. The CRQ is submitted to a CA.
5. A CA validation agent validates the content of the CRQ, including the subject information. If the certificate is intended to identify the subject, the agent or other authorized representative must manually validate the identity of the subject.
6. The CA signs the CRQ with the CA private key to produce a certificate.
7. The certificate is installed at the client and associated with the private key.

Note : by the end of the system setup phase each e-cheque's client holds a valid digital certificate. Each client holds a pair of asymmetric key that represents his digital identity in the e-cheque system.

Client Registration : A client (payer/payee) must register his digital identity at an e-cheque bank provider. After the client has registered his identity he becomes an owner of an e-cheque account. The scenario for obtaining an e-cheque account is as follows :

1. The client connects to an e-cheque bank provider.
2. The bank accepts the connection request.
3. The bank and the client exchange their digital certificates.
4. The bank and the client authenticate each other using challenge response messages through the exchanged digital certificates.
5. The bank generates its own symmetric key as secure session key and sends it encrypted to the client using the client's public key.
6. The client generates his own symmetric key as secure session key and sends it encrypted to the bank using the bank's public key.
7. The client sends a "create e-cheque account" request to the bank encrypted by the bank's session key.
8. The bank decrypts and validates the e-cheque account request according to the bank e-business rules.
9. The bank creates an e-cheque account for the client and stores the client's e-cheque account information on the bank's server.
10. The bank sends a "created e-cheque account" acknowledgement (message) to the client encrypted by the client session key.
11. The bank and the client close the connection channel.

Note: all the exchanged messages are recorded, encrypted using the destination session key, hashed with a hash function and signed using the source private key to comply with the security requirements. By the end of the client registration phase, the registered client will be the owner of an e-cheque account at an e-cheque bank provider. Now the client can withdraw or deposit e-cheques.

E-Cheque Payment

Any two clients can exchange any number of e-cheques as follows :

1. The sending client obtains the IP address of the receiving client by searching through the e-cheque network.
2. The sending client sends a connection request to the receiving client.
3. The sending and receiving clients exchange their digital certificates.
4. The sending and receiving clients authenticate each other using challenge response messages from the exchanged digital certificates.
5. The sending client generates a symmetric key as a secure session key and sends it to the receiving client encrypted using the receiving client's public key.
6. The receiving client generates a symmetric key as a secure session key and sendsit to the sending client encrypted using the receiving client's public key.
7. The sending and receiving clients exchange e-business data encrypted using each other's session key.

8. The sending and receiving client agree on a final e-business data.
9. The sending client sends an e-cheque payment request to the receiving client encrypted using the receiving client's session key.
10. The receiving client decrypts and validates the e-cheque payment request, and accepts it according to the agreed e-business data.
11. The receiving client sends a message indicating acceptance of the e-cheque payment request, encrypted using the sending client's session key.
12. The sending client encrypts one or more of his e-cheque object(s) using the receiving client's session key, and sends it to the receiving client.
13. The sending client decrypts and validates the received e-cheque object(s).
14. The sending client generates an acknowledgement for the received e-cheque(s) and e-business data and sends it encrypted using the sending client's sessionkey.
15. The sending client decrypts and validates the received acknowledgement and stores it.

Note : all the exchanged messages are recorded, encrypted using the receiving client's session key, hashed with a hash function and signed by the sending client's private key to comply with the security requirements.

E-Cheque Deposit : The client (customer/merchant) can deposit an e-cheque object into his e-cheque account at his e-cheque bank provider.

1. The client connects to an e-cheque bank provider.
2. The bank accepts the connection request.
3. The bank and the client exchange their digital certificates.
4. The bank and the client authenticate each other using challenge response messages from the exchanged digital certificates.
5. The bank generates its own symmetrickey as secure session key and sends it encrypted to the client using the client's public key.
6. The client generates its own symmetric key as secure session key and sends it encrypted to the bank using the bank's public key.
7. The client creates an e-cheque deposit request (ECDR) and sends it to the bank encrypted using the bank's session key.
8. The bank decrypts and validates the deposit request, and accepts it according to the bank e-business rules.
9. The bank sends a message indicating acceptance for the deposit request to the client, encrypted using the client's session key.
10. The client decrypts and validates the received acceptance message.
11. The client selects one or more e-cheque object(s) and sends it to the bank encrypted using the bank's session key.
12. The bank decrypts and validates the received e-cheque object(s).
13. The bank starts the cashing process of the received e-cheque object(s) according to the characteristics of each e-cheque object.