THE STATE-OF-THE-ART PRACTICES OF THE INTERNET BANKING IN TAIWAN

Ling-Yu Lin[1], Jing-Jang Hwang[2], Jung-Bin Li[2], Min-Hua Shao[2]

[1]EDP Center, Directorate-General of Budget,
Accounting and Statistics Executive Yuan
2, Gwang Zhou St., Taipei, Taiwan
Tel/Fax: +886-223823763/+886-223832580
e-mail: 2114@dgbas.gov.tw

[2]Institute of Information Management,
National Chiao Tung University
1001 Tah Hsueh Rd., Hsinchu, Taiwan
Tel/Fax: +886-35712121x57419/+886-35723792
e-mail: {jjhwang, jbli, vanessa}@spring.iim.nctu.edu.tw

ABSTRACT

This paper reports an investigation into the state-of-the-art practices of Internet banking in Taiwan. Emphasis is focused on the adoption of security technology. Three kinds of security utilities—SSL, SET, and Non-SET—are compared in terms of risks and supported functions. The author also analyzes factors that influence the development of Internet banking.

The Ministry of Finance of the Taiwanese government has adopted a policy that fosters the development of Internet banking. However, understanding security technologies demands in-depth expert knowledge, and goes beyond the capacity of general citizens. The authors suggest that the first priority is given to the authority's promulgation of laws and guidelines. Second, the banking industry needs to integrate the security mechanisms of Internet banking services with the existing environment. Finally, a risk allotment policy would help to remove fear and doubt from customer's minds.

Keyword: Electronic commerce, Internet banking, information security, transaction security

1. INTRODUCTION

As the digital era comes, the application of information technology (IT) has been a competitive advantage for businesses to increase sales and to make strategic decisions. The financial industry is an early adopter of IT, and presently the prosperity of the Internet opens a new battlefield for all banks. Traditionally banks increase their profitability by running new branches, automatic teller machines (ATMs), and telephone banking services. Herein the Internet banking service is a new option for the bank client. Being featured by 24-hour non-stop and teller-less services, the Internet banking increases business efficiency with reduced maintenance cost; hence the financial industry may have greater profit and competitive advantage.

The boom of Internet and the maturity of technology realize the application of Internet banking. The first available Internet banking institution, the "Security First Network Bank" (SFNB), initiated its service in October 1995. SFNB is also the first virtual bank on the Internet. One of its organizers Dr. Ralph Kimball states, "It is not the value of a virtual bank to threaten traditional banks, but to prove the practicality of Internet banking". The active participation of the financial industry has proved the Internet banking as a potential channel in the future.

The Internet and electronic commerce will play important roles in business in the 21st century, and their impact to the financial industry will be far greater than that to consumer products. The integration of cash flows is a critical success factor for either business-to-business (B2B) or business-to-consumer (B2C) electronic commerce. Namely the Internet banking service will help the development of businesses in the field of electronic commerce.

1.1 Motivation and Objectives

As the Internet application becomes a fast developing trend, the Ministry of Finance (MOF) authorizes Internet banking services step by step. The first authorized services include enquiries of personal account and financial information; the account transfer of registered accounts is then provided afterwards. From May 2000, the account transfer of unregistered accounts is also available. To date Internet banking services vary in several ways. The client no longer needs to go to the bank teller in order to do transactions.

According to a survey made by CitiBank, the average cost of a transaction processed by the bank teller, telephone banking service, ATM, or Internet banking service is 34, 17, 9 and 3 New Taiwan Dollars (NTD), respectively. Regardless of the difference in setup costs, the Internet banking service is still the service channel with lowest cost. The low cost encourages the financial industry to invest, but security issues discourage the client to do transactions online. The Quality of Banking Service Survey 2000 initiated by Business Weekly reveals that only 4.8% of the 5200 bank clients interviewed have Internet banking account, and 51.1% of the client without Internet banking accounts have security concerns. Hence transaction security has been considered seriously as an important factor in the development of Internet banking.

As transaction security issue is the main factor discouraging the bank's client, this paper collects information and surveys

the current state to make suggestions for the competent authority and the financial industry. We wish that a win-win situation could be achieved for both the client and the financial industry in the field of Internet banking.

1.2 Research Method

The research method of this paper is shown in Figure 1. We first design the subject matter according to our research motivation and objectives. The information source is mainly based on web sites constructed by the financial industry. An analysis, compiled based on service items, security mechanisms, and other related information, is also included. Finally a few suggestions are proposed to the competent authority and the banking authority.

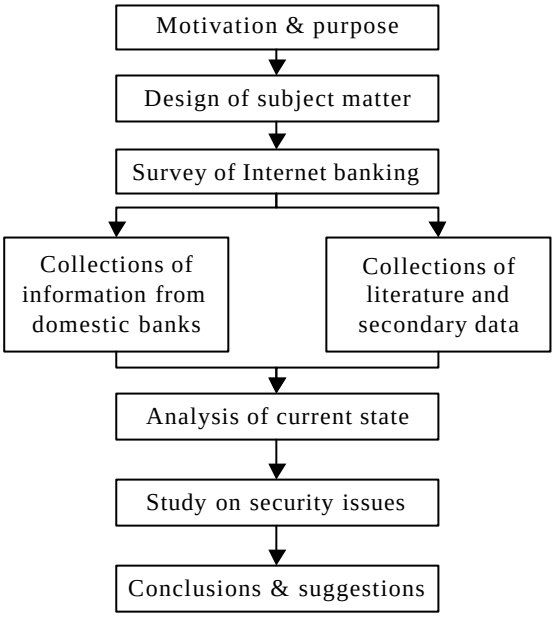

Fig. 1. Research method

2. LITERATURE REVIEW

2.1 Essentials of Internet Banking

The notion of remote banking was first proposed in the United States in 1970s, when the banks offer clients telephone services to make account balance enquiries, payments or transfers. Clients no longer had to ask for financial services at the bank counter. In early 1990s, some banks began to adopt the new PC-version family banking services. As computer and network technology become more advanced, banks offer automated devices to extend service hours and to expand service coverage area. By offering electronic financial services, the bank may benefit from cost saving, increased service efficiency, reduced branch workload, and better profitability.

There are various electronic financial services offered by the financial industry. This paper summarizes the common terms below:

Electronic Banking. The clients of financial institutions, including the natural person and the corporate person in law, may access financial services via electronic and communication devices without going to the institution. The channel of communication can be categorized into three kinds of networks: the proprietary network, the Value Added Network (VAN), and the Internet.

PC Banking. The client gets services directly from the bank by connecting his or her PC to the bank server via the proprietary bank network or the VAN. Users of PC banking may include business enterprises and individuals.

Internet Banking. The client gets services directly from the bank by Internet connection to the bank. It is not necessary to make service requests at the bank teller.

Phone Banking. The client first makes a connection to the bank server via the telephony network, and then requests for services. A dual frequency touch-tone telephone is required to access the phone banking services.

Mobile Banking. The client uses his or her mobile phone to make enquiries, transactions, or active notification services. In comparison to phone banking services, the mobile banking service takes advantage in LCD-displayed transaction process and itemized operation procedure without lengthy voice instructions.

2.2 Architecture of Domestic Internet Banking Systems

There are three participants in domestic Internet banking architecture: the bank, the client, and the Certification Authority (CA). Figure 2 illustrates the Internet banking architecture. System operation is stated as follows.

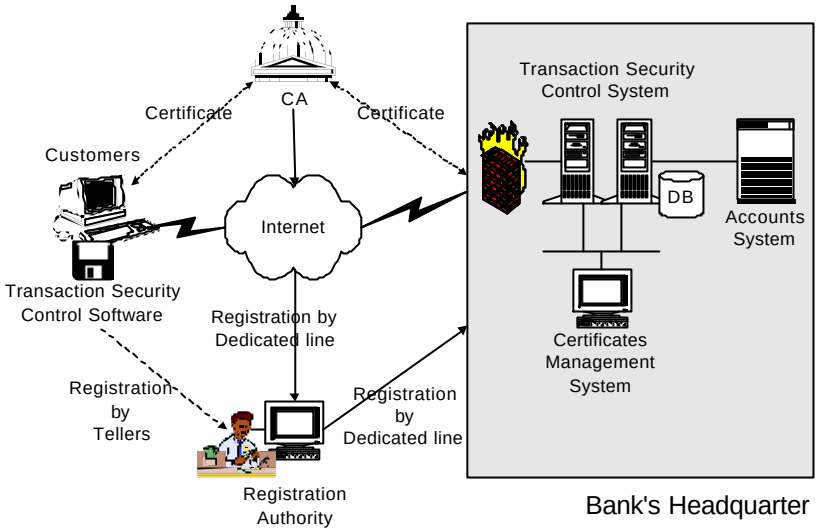

Fig. 2. Illustration of the Internet banking infrastructure
Source: Market Intelligence Center, Institute for Information Industry, 1999

If the bank client intends to access Internet banking services, he or she has to apply for an electronic certificate at one of the branches. The client will then receive a password and a floppy disk or an IC card after successful registration. The floppy disk contains a certificate application software. The client connects his or her computer with the Internet, and then applies for a certificate from the CA's web site. After CA and bank's authorization, a public key pair is generated and the private key of the key pair is stored on the client's floppy disk. The client can then access Internet banking services with this key pair and certificate afterwards.

As to the software and hardware requirements of the Internet banking services, the client needs a personal computer with capability of Internet connection, and the bank connects traditional mainframe computer with the transaction server to complete fund transfer and payments. The Internet banking service offers only those items that are appropriate to proceed over the public network. By straightforward and ease-of-use network interface, the Internet banking enables the customer to enquire his or her account balance, transaction history log, fund transfer, notification, announcement, financial products and other related information.

2.3 Security Requirements of Domestic Internet Banking Service

As fund transfer is involved in the Internet banking services, it is a critical issue to ensure transaction security. The Bankers Association of ROC (Taiwan) announced the "Security and Management Criterion for Electronic Banking of Financial Institutions" in 1998, with the permit of the MOF. This guideline describes security standard and the design of Internet banking services to secure the transactions between the client and the bank.

For better compatibility with the international security policy of electronic finance, the ROC Association of Banks and the MOF decided to revise the "Security and Management Criterion for Electronic Banking of Financial Institutions" in August 2000. The revision of the Internet banking security requirement is summarized as follows:

Security requirement of transactions: The "Security and Management Criterion for Electronic Banking of Financial Institutions" exemplifies the Internet transaction security as Table 1. According to the protection level and transaction type, the guideline classifies security requirement into two categories: mandatory and conditional. Mandatory properties must be satisfied by every Internet banking service; while the conditional ones can be optional, based on each bank's own decision.

Table 1. Security requirements of the Internet banking transaction

Category of Transaction / Property	Electronic Fund Transfer (EFT) and Transaction Instructions		Non-EFT and Transaction Instructions
	High Risk Transactions	Low Risk Transactions	
Message Confidentiality	Mandatory	Mandatory	Conditional
Message Integrity	Mandatory	Mandatory	Conditional
Authentication of	Mandatory	Conditional	Conditional

Message Origin			
Prevention of Replay Attacks	Mandatory	Mandatory	Conditional
Non-repudiation of Origin	Mandatory	Conditional	Conditional
Non-repudiation of Delivery	Mandatory	Conditional	Conditional

Exposition:

1. EFT and transaction instruction: service items regarding to fund transfer or items effecting the client's right, e.g., account transfer, remittance, payment delivery, issuance of documentary letter of credit, and modification of documentary letter of credit.
2. Non-EFT and transaction instruction: service items that have nothing to do with fund transfer or have no effect on the client's right.
3. High-risk transaction: those EFT and transaction instructions that have significant influence on the client's right, e.g., EFT of unregistered accounts or transaction instructions
4. Low-risk transaction: transactions such as account transfer of registered account, or small amount transfer of unregistered account (maximum amount: 50000 NTD/transaction, 100000 NTD/day, 200000/month). Such EFT and transaction instructions have only minimum security requirement, but security mechanism of higher level may be adopted.

Source: The Security and Management Criterion for Electronic Banking of Financial Institutions, MOF, 2000

Security requirement of management: As described in the "Security and Management Criterion for Electronic Banking of Financial Institutions", the financial institution should follow certain guidelines in Table 2. This guideline emphasizes the protection of the computer resources in financial institutions over intrusion from external channels. It also secures the integrity and confidentiality of resources, and maintains the usability of computer systems.

Table 2. Security requirements of management

Protection facility	Objectives
Complete security strategies	Only the authorized clients can access the system resource. This facility reduces the possibility of illegal intrusion.
Enhance system reliability	By enhancing the reliability and usability of the computer system, the clients may benefit from minimum possibility of unavailable services.
Organize operation management guidelines	The operation management guidelines include two separate parts for the financial institution and the client; they assure accountability, authorization procedure and responsibility attribution among financial institutions.

Source: The Security and Management Criterion for Electronic Banking of Financial Institutions, MOF, 2000

2.4 Categories of Domestic Secure Internet Banking Mechanisms

According to the "Security and Management Criterion for Electronic Banking of Financial Institutions", the security mechanisms of the Internet banking services include the following three:

Secure Sockets Layer (SSL): SSL was first proposed by Netscape in Oct. 1994. It is one of the major secure communication protocols applied on the WWW, which satisfies the basic security requirement for commercial transaction message exchange. SSL provides point-to-point authentication, confidentiality of communication, information integrity, and optionally point-to-point authentication. As SSL is one of the most popular security mechanisms on present electronic commerce transaction platform, the MOF of Taiwan demands low risk transactions in the revised "Security and Management Criterion for Electronic Banking of Financial Institutions" with symmetric key length of equal to or greater than 128 bits. The transaction with low risk is defined as which does not satisfy the properties of non-repudiation of origin and non-repudiation of delivery in electronic fund transfer and payment instruction. With additional security mechanisms such as personal identification number (PIN) and user password, the Internet banking service is better protected from malicious network attackers. It is the financial industry's own discretion to adopt appropriate mechanism based on transaction security and practical operation efficiency.

Secure Electronic Transaction (SET): SET is designed as an adaptation security mechanism for credit card payment over the Internet. It includes four groups of participants: the client e-Wallet software, the merchant server, the payment gateway, and the certification authority. Its security features protect on-line transactions in many ways. By individual application of digital certificate, the client can be authenticated. Digital signatures achieve information integrity and non-repudiation, and the digital envelope protects data confidentiality.

Non-SET: Because SET adopts detailed and complicated specifications, some banks regard the SET transaction process

as a lengthy procedure with high setup cost. Hence the financial industry designs another secure transaction mechanism, which adopts the electronic certificate and the digital signature. The Non-SET mechanism satisfies mutual authentication, information integrity, non-repudiation with the cryptographic Triple-DES algorithm to fit the security requirement of the Internet banking service.

3 CURRENT STATE OF DOMESTIC INTERNET BANKING

3.1 Evolution of Domestic Internet Banking Services

The Internet banking service grows with the maturity of network technology and the popularity of the Internet. According to a survey held by the Institute for Information Industry, the Internet population in Taiwan was 5.94 million in September 2000. AC Nielsen released a similar result that there were over 5 million Internet users by September 2000. Both surveys reveal a trend that the Internet is consistently attracting more attention in Taiwan. Presently all Internet banking services have to be permitted by the authority, the MOF. The development of the Internet banking services in Taiwan to date is depicted in the following periods:

Introductory stage (1995 to 1997). In May 1994, the MOF authorized services including enquiry, general correspondence and financial information services. The financial industry may offer these services without separate application to the authority MOF. At the time Internet user population did not reach an economic scale, thus the target achievement of offering such services was to create public acknowledgement. Services offered include general enquiries (e.g., saving deposit interest rate and currency exchange rate), account applications (e.g., application form download), and spreadsheet examples (e.g., examples of loan interest charge or term deposit interest rate).

Takeoff stage (1998 to 1999). The MOF further authorized the financial industry to run the account transfer of registered account service in January 1998. Later in May 1998 the authority announced the "Security and Management Criterion for Electronic Banking of Financial Institutions", modeling the security standards and design of services. The basic requirements such as confidentiality, integrity, authentication, non-repudiation and replay attack prevention must be achieved to secure electronic transactions. There was a boom of Internet user population in this period, and on-line shopping was drawing great attention to Internet users. The financial industry followed this trend, expanding web services and upgrading hardware peripherals to take early entry advantage. At this stage, the Internet banking service included general enquiry, account legend information, and account transfer of registered account.

Competition stage (2000 to 2001). In May 1999, the MOF released the "Guidelines Governing the Off-the-bank Automatic Service Machines of Financial Institutions". This template was to strengthen the security control operation of the financial industry and to secure the rights of the service user. Hence it clarified the rights and responsibilities between the bank and the service user for the account transfer of unregistered account. The Financial Information Service Co., Ltd. (FISC) was authorized to set upthe IEBS in February 2000, offering the financial industry a transaction platform for the account transfer of unregistered account service. The electronic commerce was growing prosperously during this period. A large-scale Internet survey held by Yam, a well-known portal site, showed that the amount of single transactions were averaging 2,611NTD, which was a prominent increase compared to past surveys. By the end of year 2000 many banks were authorized to offer Internet banking services. Herein the warfare era began with the competition among the domestic financial industry.

3.2 A survey of the current state

Survey procedure. This survey focuses on the domestic financial industry, and it collects information from the web sites set by the banks. Additional information from academic reports and other secondary information resources are also cited for analysis. The procedure of this survey is shown below:

1. Survey target: This survey investigates the top 20 banks with highest deposit outstanding. The sum of deposit outstanding of these 20 banks is over 75% of the outstanding of all banks. Table 3 lists these 20 banks.
2. Design of subject matter: Based on the motivation and purpose of this survey, the following factors are chosen as the survey subjects:
   - Presence of web site: Whether a web site has been set up to offer the Internet banking services.
   - The category of services: By distinguishing different client demands, the Internet banking services can be categorized into three groups: enquiry (e.g., account balance enquiry, transaction log enquiry, and general financial information enquiry), account management (e.g., intrabank account transfer, interbank transfer of registered account, interbank transfer of unregistered account, and transfer of tax), and others (e.g., electronic mail, application for ATM card/credit card, and lost or stolen report).
   - Security mechanisms: The "Security and Management Criterion for Electronic Banking of Financial Institutions" divides the Internet banking transactions into two groups; one is Electronic Fund Transfer (EFT) and transaction instruction, and the other is Non-EFT and transaction instruction. Because of their different security requirements, this survey analyzes their mechanisms respectively.
   - Transaction system implementation: Summarizes the implementation state of the Internet banking services. The banks may build their own transaction platform, or adopt the FISC' s Internet Electronic Banking System (IEBS).
3. Duration of survey: From December 2000 to March 2001.

Table 3. Listing of the Internet banking services

Rank	Bank	Enquiry			Account Management				Others				URL
		Account balance	Transaction log	General financial info	Intrabank account transfer	Interbank transfer of registered account	Interbank transfer of unregistered account	Transfer of tax	Electronic mail	ATM card application	Lost or stolen report	Credit card business	
1	Bank of Taiwan	*	*	*	*	*	*	*		*	*	*	www.bot.com.tw
2	Taiwan Cooperative Bank	*	*	*	*	*	*	*		*	*	*	www.tcb-bank.com.tw
3	Land Bank	*	*	*	*	*	*	*		*	*	*	www.landbank.com.tw
4	First Commercial Bank	*	*	*	*	*	*	*	*	*	*	*	www.firstbank.com.tw
5	Hua Nan Commercial Bank	*	*	*	*	*	*	*	*	*	*	*	www.hncb.com.tw
6	Chang Hwa Bank	*	*	*	*	*	*	*		*	*	*	www.chb.com.tw
7	Taiwan Business Bank	-	-	*	-	-	-	-	-	-	-	-	www.tbb.com.tw
8	Chinatrust Commercial Bank	*	*	*	*	*	*					*	www.chinatrust.com.tw
9	United World Chinese Commercial Bank	*	*	*	*	*	*	*				*	www.uwccb.com.tw
10	The International Commercial Bank of China	*	*	*	*	*	*	*	*	*	*	*	www.icbc.com.tw
11	Taipei Bank	*	*	*	*	*	*	*			*	*	www.taipeibank.com.tw
12	The Farmers Bank of China	*	*	*	*	*	*	*	*		*		www.farmerbank.com.tw
13	The Shanghai Commercial and Savings Bank	*	*	*	*	*			*		*	*	www.scsb.com.tw
14	International Bank of Taipei	*	*	*	*	*	*	*				*	www.ibtpe.com.tw
15	Hsinchu International Bank	*	*	*	*						*	*	www.hibank.com.tw
16	Chiao Tung Bank	*	*	*							*		www.ctnbank.com.tw
17	Bank of Overseas Chinese	*	*	*									www.booc.com.tw
18	Taishin Bank	*	*	*	*	*	*	*	*		*	*	www.taishinbank.com.tw
19	Fubon Bank	*	*	*	*	*	*		*			*	www.fubonbank.com.tw
20	E.Sun Commercial Bank	*	*	*	*	*	*		*			*	www.esunbank.com.tw

Summary of this survey: The information collected in this period is described below.

1. Service items: Table 3 summarizes the services offered by the top 20 banks. Asterisk "*" represents available services, blank " " represents services unavailable, and dash "-" means information not available. This survey shows that all 20 banks provide general enquiry services. Because of the membership policy of the Taiwan Business Bank, service information other than general enquiries is not accessible. 12 out of the remaining 19 banks provide complete account management services. 2 (Chiao Tung Bank and the Bank of Overseas Chinese) of the other 7 banks provide no services in this category. As to other services, this survey focuses on electronic mail service, banking card application, lost/stolen card report, and credit card application. Among all services, credit card application is the most common service, which is provided by 16 banks. 8 banks offer electronic mail delivery of statement or other passbook-related information. Banking card application and lost/stolen card report are provided by 7 and 13 banks, respectively. This survey explains a fact that the domestic financial industry is playing an active role in implementing Internet banking services. So far the service items offered among banks have no substantial difference, and they are estimated to be uniform. Hence for the financial industry, the Internet banking service will be general and ordinary service instead of particular competition advantage.
2. Transaction system: As the security requirement varies on different services, the financial industry adopts security mechanisms of several levels. The mechanisms used in the Internet banking services, categorized earlier as SSL, SET and non-SET, are shown in Table 4. SSL is commonly used for enquiry, low risk account management services and other service items with security concern. SET and non-SET mechanisms are adopted for account transfer services. At present the financial industry may choose to build its own platform or to import FISC's IEBS to provide account management services.

Table 4. Usage of security mechanisms for the Internet banking services

Service / Security Mechanism	Enquiry		Account management		Other services
	General information	Account balance	Low risk transaction	High risk transaction	
SSL		✓	✓		Optional
SET			✓	✓	
Non-SET			✓	✓	

Table 5 shows the implementation state of the account transfer transaction system for the Internet banking service. In the 20 banks offering the Internet banking service, the Taiwan Business Bank is not accessible due to its membership policy (5% of all the 20 banks). 14 out of the 20 banks adopt FISC's share Internet banking system (70%); 3 banks (15%) do not use IEBS, including Chinatrust Commercial Bank (non-SET system), Shanghai Commercial and Savings Bank (128-bit SSL system for account transfer service), and Hsinchu International Bank (128-bit SSL system for account transfer service). 2 banks (10%) have no account transfer system.

A finding of this survey reveals that the majority (14 out of the 20 banks) of the domestic financial industry adopts FISC's IEBS for account transfer transactions. However, 9 of these 14 banks also implement other account transfer transaction system. Clients of these banks may choose their preferred transaction platform. In the case of Hua Nan Commercial Bank, it offers 3 systems for interbank account transfers, including FISC's IEBS, its non-SET system, and the 128-bit SSL system. As the service charge varies with the chosen transaction system, platform selection can possibly be confusing for the client. Such a chaotic situation is attributed to the low degree of integration between the FISC's IEBS and the financial industry's internal systems.

The certificate of IEBS is registered with the bank client's account number, somehow this client may have more than one account within the bank, such as demand deposit account, checking and savings account, time deposit account, etc. Authentication based on single-account certificate leads to a troublesome situation that the client has to apply for many certificates, and each account needs a unique certificate. With keen competition in the banking industry, the Landbank offers revised Internet banking service in May 2001. The certificate is registered with the client's citizen ID instead of one account number in this revision; hence the client may use this certificate to make transactions with any of his or her account.

In addition to the essential security requirements, the financial industry also evaluates the practical factor of system integration for better service quality. Hence this will be a major issue of the financial industry in the near future.

Table 5. Implementation state of the account transfer transaction system

Bank	Platform	Internet banking account number	Security mechanism	Available institutions for EFT	Service charge (intra-bank/ inter-bank)
Bank of Taiwan	IEBS	Demand deposit account number	SET	Members of IEBS	10/15
Taiwan Cooperative Bank	IEBS	Demand deposit account number	SET	Members of IEBS	Free/12
Land Bank	IEBS	Demand deposit account number	SET	Members of IEBS	5/15
First Commercial Bank	IEBS	United account number for all accounts	SET	Members of IEBS	7/15
Hua Nan Commercial Bank	IEBS	United account number	SET	Members of IEBS	10/15
	Individually-built system		Non-SET	Members of FISC' s shared CD/ATM system	Free/15
			SSL 128bits	Members of FISC' s shared CD/ATM system	Free/15
Chang Hwa Bank	IEBS	United account number	SET	Members of IEBS	Following FISC' s charging policy
	Individually-built system		SET	Partial financial institutions	
Taiwan Business Bank	-	-	-	-	-
Chinatrust Commercial Bank	Individually-built system	United account number	Non-SET	Members of FISC' s shared CD/ATM system	Free/18
United World Chinese Commercial Bank	IEBS	United account number	SET	Members of IEBS	Free/18
	Individually-built system		SSL	Members of FISC' s shared CD/ATM system	
The International Commercial Bank of China	IEBS	Demand deposit account number	SET	Members of IEBS	-
Taipei Bank	IEBS	Demand deposit account number	SET	Members of IEBS	Free/18
	Individually-built system		SET		
The Farmers Bank of China					
The Shanghai Commercial and Savings Bank	Individually-built system	Composite account number	SSL 128bits	Members of FISC' s shared CD/ATM system	Free/18
International Bank of Taipei	IEBS	United account number	SET	Members of IEBS	Free/15
	Individually-built system		SSL 128bits	Members of FISC' s shared CD/ATM system	
Hsinchu International Bank	Individually-built system	United account number	SSL 128bits	Bank of the account holder	Free

Bank	Platform	Internet banking account number	Security mechanism	Available institutions for EFT	Service charge (intra-bank/ inter-bank)
Chiao Tung Bank					
Bank of Overseas Chinese					
Taishin Bank	IEBS	United account number	SET	Members of IEBS	Free/18
Fubon Bank	IEBS	Demand deposit account number	SET	Members of IEBS	Free/15
	Individually-built system		SSL 128bits		Free/18
E.Sun Commercial Bank	IEBS	United account number	SET	Members of IEBS	Free/18
	Individually-built system		SSL 128bits	-	-

3. Security mechanisms: Following the "Security and Management Criterion for Electronic Banking of Financial Institutions", the financial industry offers enquiry and other non-EFT services without mandatory usage of electronic certificates. Instead, the client is asked to sign in by the user identification number and password. Messages transmitted over the Internet are encrypted by SSL to enhance security. If the login procedure fails 3 times consecutively, the client has to apply for another valid password. To further strengthen security control, the Internet banking system terminates a user session after the client idles over 5 minutes in this system.

   Three security mechanisms protect the account management services, which are in the category of the EFT and payment instruction service.

   - 128-bit SSL encryption: The "Security and Management Criterion for Electronic Banking of Financial Institutions" suggests that the EFT and payment instructions of account management services have to satisfy non-repudiation of delivery and non-repudiation of reception. Further, the key length of adopted symmetric cryptosystem should no less than 128 bits. The financial industry chooses the 128-bit SSL product along with password sign-in. In this survey, there are 7 banks out of 20 adopt such system.
   - SET: As it is tailor-designed for credit card payments on the Internet, the financial industry uses it with some modification. The Internet banking system concatenates the account number, the identification number of bank, and the application serial number as the client's SET credit card number. The participants of this system include the client (cardholder in SET), the bank (merchant in SET, may be the financial industry or FISC), the clearing center (acquirer in SET, may be the financial industry or FISC), the bank (issuer in SET), and the certification authority. The Internet banking system takes advantage of the security protocol and data format of SET to gain customer acceptance of on-line transactions.
   - The IEBS of FISC is secured by SET, and it is adopted by 14 banks. In addition to IEBS platform, the financial industry also implements its own transaction platforms. Chang Hwa Bank has both FISC's IEBS and its own SET system for account transfer services.
   - Non-SET: The financial industry implements security mechanisms other than SSL and SET for its individual need. At present the Taiwan-CA company (TaiCA) offers certification service for these non-SET Internet banking systems. The electronic certificate and digital signature provide user authentication, data integrity, and non-repudiation protection along with additional encryption of triple-DES. The non-SET system specification provided by TaiCA is similar to SET, but it is without the involvement of the third party (e.g. FISC) to fit the interaction model between the client and the bank. A comparison of the two is shown in Table 6. Presently 3 banks, Chinatrust Bank, Hua Nan Commercial Bank and Land Bank implement non-SET systems.

Table 6. Comparison of SET and non-SET systems

Item	Internet Electronic Banking System of FISC (SET)	Non-SET transaction system
The Security and Management Criterion for	Message confidentiality, integrity, authentication, replay attack prevention,	Message confidentiality, integrity, authentication, replay attack prevention,

Electronic Banking of Financial Institutions	and non-repudiation and delivery and receipt	and non-repudiation and delivery and receipt
Content of certificate	Account number	Citizen ID
Authentication	Client/IEBS/bank follow the cardholder/merchant/bank authentication procedure of SET	Mutual authentication of client/bank
Operating system	The bank website is a transaction window only; FISC handles real transactions	Individual platforms implemented by bank; simplified operation procedure with higher system integration
Software requirement of the client	Authorized SET e-Wallet software installation; private key and personal certificate have to be stored in hard drive	"Client management software" installation; private key and personal certificate are stored in floppy disk

3.3 Customer Acceptance of Internet Banking Services

The Quality of Banking Service Survey 2000 initiated by Business Weekly interviewed 5200 bank clients, only 4.8% of the interviewees have Internet banking account. The reasons not to take Internet banking services include security concern (51.1%), habit of interpersonal contact (45.1%), and sufficient convenience of ATM machines (over 30%).

This survey further analyzes dissatisfaction factors from the 247 clients with Internet banking accounts among all 5200 interviewees. The most dissatisfaction factor is attributed to the slow speed of enquiry (33.2%); other 2 noticeable factors are frequent connection failure (27.1%) and lack of user-friendly interface (over 10%).

As the financial industry evaluates the Internet banking service as the mainstream in the future, implementation of transaction system will be consistently going ahead. However the growth of the Internetbanking client is not substantial yet, baffled by the issue of transaction security. Although the Internet infrastructure is not mature in Taiwan, and the age of heavy Internet users does not fit the target market of the financial industry, the e-generation at the age of 20 to 30 will still be the key client of the Internet banking services in future.

4. ANALYSIS OF TRANSACTION SECURITY

The Internet banking system provides services in the public network, hence the account holder's equity is vulnerable to the lack of security protection. The transaction message transmitted may suffer from eavesdropping, modification, malicious deletion, fabrication of message or identification, repudiation of bank or client, or even invasion of system. Transaction delay and error are other reasons to cause the account holder's loss. These threats lower the account holder's will to choose Internet banking services. Thus the security issue is a major concern by both the client and the bank. Security requirements may be achieved by cryptographic mechanisms and comprehensive system design and management. Herein the current state of cryptographic products and the related protocols such as SSL, SET and non-SET security mechanisms are further elaborated below:

4.1 Cryptography

Symmetric and asymmetric cryptosystems: To ensure the confidentiality of communication, information is first encrypted into ciphertext before transmitting to the receiver. The legitimate receiver uses the same cryptographic algorithm to convert ciphertext back to plain text. Two types of cryptographic mechanisms are in use: the symmetric and asymmetric cryptosystems. The symmetric cryptosystem is also addressed as secret key cryptosystem, in which the message sender and receiver use the same key to encrypt/decrypt messages. Data Encryption Standard (DES) is the most widely used symmetric cryptosystem.

The other type of cryptosystem is asymmetric, known as public key cryptosystem. Every participant of this system uses a pair of keys for message encryption/decryption respectively. These two keys (one public key, one private key) have a mathematical relation, and it is futile trying to compute a private key from the corresponding public key. Namely, the announcement of public key does not damage the confidentiality of the corresponding private key. Asymmetric cryptosystems are commonly used for message encryption/decryption and generation of digital signatures. RSA is the most widely used asymmetric cryptosystem.

Digital signature: Digital signature is an application of the public key cryptosystem. The sender uses his or her own private key to encrypt messages, and the outcome of encryption is a digital signature. The message receiver uses the sender's public key to verify the signature and to secure message integrity.

Message Authentication Code (MAC): In business activities, both the message sender and the receiver concern if there is malicious modification of message. One-way hash function is adopted in this matter, and it helps to compute message digest MAC. Message of arbitrary length is hashed into a fixed-length MAC. It facilitates the system processing, because digital signature is more efficient by encrypting the message digest instead of original whole text. Commonly used one-way hash functions are Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA).

Digital certificate: Before proceeding transactions in the wide open Internet, all participants of the system have to authenticate one another. The characteristics of digital signature help this concern, but the major issue is to validate the legitimacy of other participants' public keys. In this case,

the job of key management has to be handled by a fair and objective organization. This organization, the certification authority (CA), manages works such as certificate assignment, filing, and revocation. Every participant of the system validates a certificate by CA's public key.

X.509 key management standard: This standard is organized by the International Telecommunication Union (ITU) and the International Standards Organization (ISO). X.509 adopts a hierarchy structure of organizations to work on user authentication and certificate issuance. The fields in a X.509 format certificate record the version, certificate serial number, algorithm, issuer name, subject name, subject's public key, period of validity, and other information.

4.2 Current State of Cryptographic Applications

The Research, Development and Evaluation Commission of the Executive Yuan entrusted Chinese Open System Association (COSA) to set the "Regulations Governing the Information Processing of Public Institutions". The evaluation regarding to the financial information security is listed in Table 9. As the level of consensus, stability, completeness, and maturity are all evaluated as high level; the infrastructure of domestic Internet banking is further consolidated.

Table 9. Security evaluation of financial information

Item	Level
Level of Consensus	High
Stability	High
Completeness	High
Maturity	High

Source: The Regulations Governing the Information Processing of Public Institutions, the Research, Development and Evaluation Commission, the Executive Yuan, ROC

5. CONCLUSION

The MOF encourages the financial industry to provide Internet banking services with protection of security and clients' equity as two prerequisites. Although the financial industry is consistently investing and implementing transaction platforms, the bank client does not have a participative response as expected. The inconvenience of SET discourages the public to adopt the whole SET architecture. In June 21, the major credit card issuers including ChinaTrust Commercial Bank announced to stop issuing SET certificates for the cardholder. Herein a critical success factor for Internet banking is attributed to the existence of a secure environment drawing the client's participation. Thus the following suggestions are summarized:

Laws and regulations: The government should play a supportive role in newly evolved business services, and it has to promulgate general principles as the guidelines for the sector's execution. Only through such approaches can the society earn the greatest welfare. For example, the MOF requests the financial industry to follow SET security standards when offering high-risk transaction services. In this case, the financial industry is faced with a holdback when adopting operational products, which violates the principle of general guidelines. Thus the development of Internet banking may be limited, and the appropriateness of legal regulation has to be reviewed time after time.

Market acceptance of security mechanisms: The phlegmatic attitude of bank clients toward SET certificate issuance mentioned above exemplifies the concerns of new network services. In addition to security issues, the Internet banking has to take care of the habit of commercial behavior and the ease of integration with existing operations. One shortcoming of SET is the certificate application and usage policy for the client. When the client has more than one bank account, the efficiency and transparency of certificates will become important issues to reduce the development cost of Internet banking.

Implementation of risk allotment policy: Practically, two factors other than transaction security are considered: the convenience of regular operation and the acceptance of the client. Taking the credit card system as an example, regardless of the large amounts of credit card thefts and frauds, it is still widely accepted by clients. A risk allotment policy protects the client with limited loss; hence the client trusts and uses this system. The competent authority secures the client equity by allotting the client's loss to the issuer bank. The MOF revised the "Standard Contract of Credit Card" in January 2001, in which the maximum loss for a loss or stolen card report is 3000 NTD. With this contract of limited loss, the cardholder increases his or her trust in making credit card payments. Similarly, the competent authority should promulgate a policy to allot potential loss of on-line transactions.

ACKNOWLEDGEMENT

This research was supported by grant NSC 89-2416-H-009-038 from the National Science Council, Taiwan.

REFERENCES

[1] Ministry of Finance. *The Security & Management Criterion for Electronic Banking of Financial Institutions*, 2000.

[2] Ministry of Finance. *Guidelines Governing the Off-the-bank Automatic Service Machines of Financial Institutions*, 1999.

[3] Ministry of Finance. *Important financial policies and*

measures, 2001. Retrieved from the World Wide Web: http://www.boma.gov.tw/english/p3.htm

[4] Executive Yuan. *Regulations Governing the Information Processing of Public Institutions*, 1999.

[5] ISO/IEC JTC 1. *ISO/IEC 10181-7 Information technology -- Open Systems Interconnection -- Security frameworks for open system*, 1996.

[6] Visa International and MasterCard International. *SET Secure Electronic Transaction Specification: Book 1. Business Description*, Version 1.0, 1997. Retrieved from the World Wide Web: http://www.setco.org/.

[7] Stallings, W. *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice Hall, 1999.

[8] Fayawardhena, C. & Foley, P. "Changes in the financial industry-the case of Internet banking in the UK," *Electronic Networking Applications and Policy*, 2000, 10(1), 19-30.

[9] Awad, E.M.. "The Structure of E-Commerce in the Banking Industry: An Empirical Investigation," *Communications of the ACM*, 2000.

[10] Skipper, J. "Electronic Banking And Payments," *The Institution of Electrical Engineers*, 1998.

[11] Clark, T.H. & Lee, H.G. "Security First Network Bank: A Case Study of an Internet Pioneer," *the Proceedings of the 31st Annual Hawaii International Conference on System Sciences*, 1998.