SECURITY OF BANKING TRANSACTIONS OVER THE INTERNET

Information technology is playing an ever increasing role in the business of banking. A Study Group on Electronic Banking was established by the Hong Kong Monetary Authority (HKMA) in July 1997 to enable it to keep abreast of developments in electronic banking and to assist in the development of appropriate policy and regulatory responses to technological developments. One of the first topics reviewed by the Study Group was the security of banking transactions over the internet. The following article is the product of the study on this topic and outlines HKMA's current understanding and position with respect to internet banking in Hong Kong.

Introduction

Developments in information technology in the last few years have popularised the use of the internet as a communications channel. The number of people actively using the internet is increasing exponentially and new types of services have been developed to take advantage of the internet as a delivery channel.

Banking conducted through the internet or *virtual banking* offers tremendous convenience to customers in managing their finances. Moreover, it is a cost efficient channel for institutions to target banking services that can be tailored to suit an individual customer's needs. However, the nature of banking transactions demand adequate security to be provided to protect both customers and banking institutions. This is irrespective of whether banking is conducted in a physical or *virtual* manner. In the case of internet banking, the ability to conduct transactions without any physical interaction does change the nature of the risks involved. The issue of security is one of the largest concerns which can inhibit widespread usage of this new technology. This article reviews a number of aspects concerning the security of banking transactions over the internet.

Specifically, this article will:

- identify the security risks involved in banking transactions conducted over the internet;
- identify and assess the options available to address these risks;
- highlight the importance of security policies and procedures as an integral part of security; and
- describe the HKMA's supervisory approach to internet banking.

Security Risks in Internet Banking

A major concern over the internet is its open nature. In relation to banking on the internet, this translates into increased risk of unauthorised access to and alteration of information. Accordingly, the fundamental objectives that internet security technology should achieve include:

- the true identity of each party to a transaction is ascertained before a transaction is conducted;
- information is transmitted only to the intended recipient and that the information received is the same as that sent by the originator; and
- unauthorised access to information is prohibited.

Although security measures have been developed to specifically address these concerns, new measures are also being developed to defeat these measures. Therefore, the development of security measures to keep up with changes in technology in order to maintain an adequate level of security is an ongoing process. Accordingly, there are still significant concerns on whether there is adequate security for transacting over the internet. This is an issue of particular importance in the context of banking where most transactions would involve transfers of value.

Banking transactions typically involve bank to customer and bank to bank transactions. However, the security risks involved are no different in nature to any other internet transactions involving a transfer of valuable information. A transaction across the internet goes through many different stages of processing and many different systems. Data would be entered on a remote computer, processed and transmitted to various internet

service providers across the internet backbone. The data is then received by the bank's firewalls, routers and web server and then forwarded to the bank's mainframe for further processing. Anywhere along this line of communication is a potential point where unauthorised access to information is possible. The general risks which could affect the security of both types of transactions include:

- false authentication of parties to a transaction;
- interception of information transmitted; and
- unauthorised access to information or systems.

These are examined below in greater detail.

False authentication

A transaction conducted through the internet does not require any face to face or other physical interaction between the parties to a transaction. This increases the difficulty in checking the identity of all parties to a transaction. There are many tools available to verify identities electronically. At present, the most common authentication method is the use of user ID and passwords. However, it is widely recognised that such systems by themselves have significant weaknesses in practice and are dependent upon the strict enforcement of password security. A more effective alternative method to authenticate parties involves the use of digital signatures together with supplementary devices such as smart cards. In addition, alternative forms of identification methods such as fingerprint, retinal or facial scanning are also available.

Interception of data transmitted

The open nature of the internet significantly lowers the difficulties of intercepting data. This is because the relevant data can pass through many computers on its journey to the final destination. This increases the number of points where interception can take place as these points may not be secure. There is currently no effective way to prevent interception of data sent via the internet. Therefore the only viable option is to ensure that information intercepted cannot be read without prior consent or authority. Cryptographic techniques which scramble or "encrypt" messages into an unintelligible form and which can only be "decrypted" with a special "key" are available specifically to address this problem.

Access to a bank's internal computer system

Unauthorised access to a bank's computer systems can be gained from within the bank's own internal network or from an outside network such as the internet. For a bank offering internet banking services, it is extremely important that intruders are prevented from accessing and modifying confidential information held by the bank. Since a bank's business relies heavily on its reputation for maintaining adequate security, any successful breach of security (whether or not confidential information was involved and irrespective of whether financial losses were suffered) would have a significant impact on a bank's reputation and adversely affect its business.

There have been many examples of supposedly secured web sites having been successfully "hacked" and their contents changed. Such sites include the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the US Department of Justice, the National Aeronautics and Space Administration (NASA), etc. News of such breaches propagates quickly with the help of the media and the adverse publicity would tend to last a long time. There is no reason why banks which advertise the high level of security in their internet banking services would not be subject to similar attacks. A fur company's web site was recently hacked to present an opposing view by anti-fur activists and banks would present attractive targets to many hackers. In Hong Kong, hacking to gain unauthorised access to any program or data held in a computer is an offence under the Telecommunications Ordinance. In more serious cases where there is criminal intent, it is a criminal offence under the Crimes Ordinance and carries a maximum penalty of 5-year imprisonment. However, given the open nature of the internet, enforcement can be a big problem. For a bank, high levels of security should not only be limited to data considered to be most sensitive or those which could result in substantial financial losses if they were disclosed. All information which would affect a bank's reputation for security soundness also requires adequate protection.

Unauthorised access from external sources

Banks that offer electronic banking services must be able to receive messages (which would include certain instructions as well as financial data) in order to effect a transaction. Therefore there must be a way to gain access into the bank's internal systems and files from outside the network. Software is commonly available either free of charge or for only nominal sums to enable access to a host computer from a remote site located anywhere in the world. On the assumption that there is no protection, commands could be sent from this remote site to control the operations or access sensitive files in an internal computer system.

The open nature of the internet is based on common communication standards and protocols. Accordingly, banks must follow these standards to allow an internet transaction to take place. These standards identify the type of data sent, the sender and recipient's computer address, the applications needed to read the data and other information that defines an internet message. These open standards, however, could be manipulated to allow unauthorised access into a bank's internal systems. For example, the code in the protocol can be changed using software to disguise a virus program such that it would appear to be an email message to the receiving computer. In order to prevent this, there must be properly configured tools to identify, restrict, and control access to areas of a bank's computer systems that contain sensitive information. Security tools such as firewalls are available to fulfill this role.

Unauthorised access from internal sources

The maintenance of adequate security to prevent unauthorised access is not a new concept introduced by internet banking. Banks should already have comprehensive measures and effective controls in place to ensure that access to sensitive information (including data and programs) is only available to authorised personnel.

The introduction of internet banking services can, however, increase the complexity and scope of the existing policies and procedures. Employees would typically have some level of access to a bank's network to allow them to perform their day to day duties. Some would even have a high degree of knowledge of a bank's security systems and the areas of weakness. The risks of loss from attacks by knowledgeable employees are much higher than outside attacks. Surveys conducted overseas indicate that internal attacks (including those from ex-employees) comprise at least 70% of all reported attacks on companies' computer systems. One of the most common methods used to gain unauthorised access is through the use of legitimate passwords obtained in a workplace where password security procedures are not strictly observed. This is of particular importance in operating systems such as Unix which many banks rely on for their main processing functions. These operating systems have a "superuser" account that allows the system administrator access to all resources, data and programs in a bank's computer. If a person gains unauthorised access to this account, he or she can effectively control all aspects of a bank's computer processing functions.

In order to maintain customers' confidence, banks need to ensure that they can distinguish between internal and external attacks. They must prevent collaboration between internal employees and outside parties to attack their computer systems. Technology is available to assist in this area. However, it is more important that banks maintain a comprehensive set of security policies and procedures that are rigorously enforced as a preventive measure against such abuses.

Security Measures

There are different types of technology available to address the risks identified above and many more are being developed. Developments in this area are ongoing because new measures to attack existing technologies are also being developed at a similar rate. Accordingly the situation on security products and methodologies is likely to continue to change quickly. Despite this, it is relevant to review the existing technologies available, their effectiveness as a security measure and how these technologies are likely to develop in the near future.

It is recognised that absolute security is not possible and that the aim should be to achieve similar levels of security to those that currently exist in conventional banking transactions. Similarly, the level of security in systems used to protect sensitive information should be comparable to that used to protect a physical location.

The risks identified above can be managed through a combination of the following:

- cryptographic techniques
- firewalls
- other measures

Cryptographic techniques

Cryptographic techniques fall into two major categories: symmetric key encryption and public key encryption. All cryptographic techniques require the use of "keys" or a set of numbers used in combination with a formula to encode and decode a message into and out of an unreadable form. This is analogous to a combination used to open a safe. The "key length" (measured in bits) would represent the length of the safe combination and is one measure of the strength of the encryption technique against attacks aimed at solving the key. This also means that, for any given algorithm, a larger key will take longer to encode and decode a message which has a performance impact. Another general characteristic is that the level of security of a key would decline in proportion with increase in time and the number of key holders.

Symmetric key cryptography

This technique employs the same key to encrypt *and* decrypt a message. Common types of symmetric algorithms include Data Encryption Standard (DES) and International Data Encryption Algorithm (IDEA). One important aspect of symmetric key encryption is that encoding and decoding can be performed very quickly. This type of algorithm also works well in a "one-to-one" situation and where the duration of the key is expected to be short. However, in a public environment such as the internet where "one-to-many" and "many-to-many" types of transactions are more prevalent, the level of security offered by symmetric keys would be very low unless a disproportionate amount of effort is put into key management and key exchange over the internet.

Public key cryptography

This technique (also called asymmetric key cryptography) requires the use of a pair of different keys commonly known as a "public" and "private" key pair. As the name suggests, the public key need not be kept secret. The private key on the other hand is *only* known to the owner of the key. Information can be encrypted using either of the keys, but it can only be decrypted using the other key in the pair. The algorithm is also designed such that it is not practicable, provided that the keys are of sufficient length, to derive the private key from the public key or vice versa. The technique is basically a mathematical function that is easy to do one-way and very hard to do in reverse. The most commonly used public key algorithm is Rivest, Shamir and Alderman (RSA). However new techniques (such as Elliptic Curve Systems) that improve both the performance and security aspects of encryption are being developed.

In order to ensure privacy of a message, the sender would use the public key of the recipient to encrypt a message (Figure 1). The recipient would then use his or her corresponding private key to decrypt the message (Figure 2). Since there is no need to exchange the private key between the two parties, this solves the problem of having to transmit the private key that is inherent in symmetric key systems. There is also a need to ensure that a particular public key belongs to the rightful owner and this is achieved through certification of the public key by a trusted party with the use of *digital certificates*. Public key cryptography is therefore a powerful tool for maintaining confidentiality of information.

Figure 1 – To Encrypt a Message

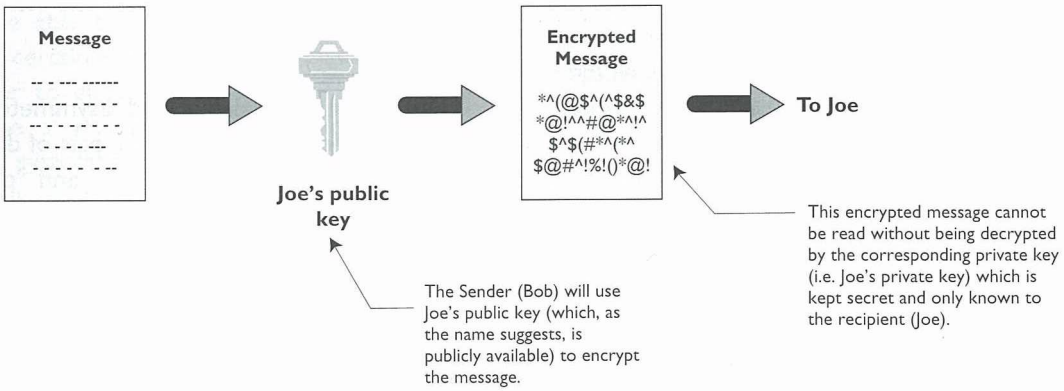
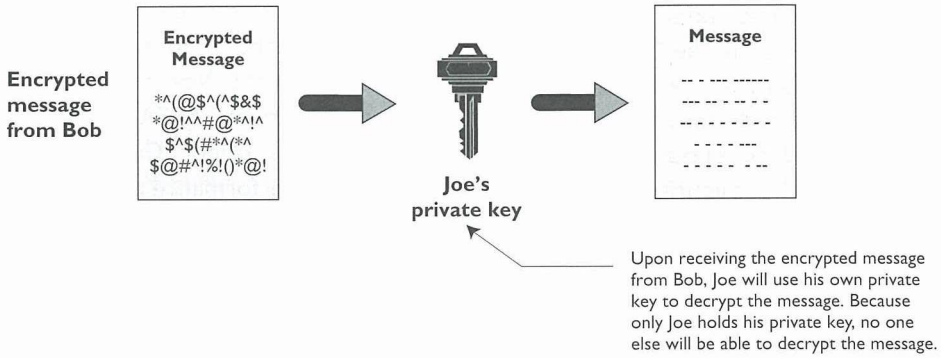


Figure 2 – To Decrypt a Message



Another important feature of public key cryptography is that it enables parties to a transaction to authenticate each other through the use of *digital signatures*. Digital signatures can be considered to be the equivalent of paper signatures. They allow the recipient of a message to check that the message was indeed sent by the rightful party[1] and that the contents of the message have not been modified in any manner. This is of course based on the fundamental assumption that the private key was kept secret by the sender. Therefore, digital signatures also enable *non-repudiation*, that is, the person that digitally signed the message cannot later deny having done so (Also see Box – Digital signatures, certificates, certificate authorities and public key infrastructures).

Although the public key concept is sound from the technical point of view, it has one major drawback —— speed. Public key systems typically have longer keys and need significantly more processing time to encode and decode messages compared to symmetric key systems (by a factor of about 100). The longer key lengths are necessary because of the need to make it impractical to derive the private key from the public key. Therefore in practice, most secured transactions will be conducted using a combination of both types of algorithms. Public keys would be used to encrypt a symmetric key for a particular session (known as session keys) and this symmetric key would normally be used for encrypting messages during the session. However, it is disposed of at the end of each session and a new session key would have to be generated at the beginning of each new session. In this way, transactions can be completed within a reasonable amount of time and in a secure manner.

1 This aspect also depends on whether access to the device used to send the message (such as a personal computer) is properly controlled as it may contain sensitive information (such as passwords and private keys) that must be kept secret.

Strength of encryption as a security measure

The most desirable assessment of security algorithms consists of a public review by as many cryptographic experts as possible in order to analyse and detect any weaknesses in the design of the encryption method. An example of this is RSA's Secret-Key Challenge where individuals, companies and other organisations were invited to break messages encrypted with 56-bit DES algorithm. If an encryption algorithm has withstood such reviews ("cryptoanalysis") for a considerable time, one can be reasonably sure that it does not contain secret "trapdoors" or undetected weaknesses. The use of public and extensively reviewed algorithms is therefore an important security principle.

The strength of encryption is not based on the secrecy of the applied algorithm since this would generally be made known to a number of parties. The strength of encryption lies in the fact that the secret or private keys are known *only* to the holder of the key. It is thus important that 1) procedures are in place to generate keys in a secured environment, 2) these keys are stored safely and 3) encryption and decryption keys of sufficient size are used. This is of special importance to a bank which would not be able to afford significant breaches of security in banking transactions or to their systems from both financial and reputational perspectives.

To assess the strength of encryption algorithms, it can be assumed that the algorithm and the encrypted text are known to an outsider. An outsider could try to discover the plain text by testing all possible decryption keys. This type of attack is known as a *brute-force attack*. The amount of processing resources needed to solve the correct decryption key through a brute-force attack for a given algorithm and a given key length can be calculated relatively easily. In the case of the RSA Secret-Key Challenge, a team of university students, programmers and scientists joined together thousands of computers over the internet and was able to crack the DES 56-bit key (which has 72 quadrillion possible keys) in around 4 months. With increasing computing power, brute-force attacks against symmetric cryptographic systems with small key lengths will be a fast and cheap way to obtain the secret keys. To provide adequate protection against the most serious threats, such as well-funded commercial enterprises or government intelligence agencies, key lengths of 128-bits are now recommended for new symmetric systems. This key length has been estimated to be adequate against brute-force attacks for the foreseeable future (around 20 years). A summary of various symmetric key lengths and the estimated time to break is shown at the table below.

The fundamental assumption behind public key cryptography is that a person must not be able to use a public key to derive the corresponding

Strength of Symmetric Key Cryptography

Strength of symmetric key cryptography based on the average time estimates for a hardware brute-force attack in 1995. Note that the absolute figures shown below would only provide a reference to indicate the relative strengths of keys with different key lengths. The increase in the processing power of computers would lead a general drop in the time to break such keys.

	Key length in bits					
Cost (US$)	**40**	**56**	**64**	**80**	**112**	**128**
100,000	2 sec	35 hours	1 year	70,000 yrs	10^{14} yrs	10^{19} yrs
1 million	0.2 sec	3.5 hrs	37 days	7,000 yrs	10^{13} yrs	10^{18} yrs
10 million	0.02 sec	21 min	4 days	700 yrs	10^{12} yrs	10^{17} yrs
100 million	2 ms	2 min	9 hrs	70 yrs	10^{11} yrs	10^{16} yrs
1 billion	0.2 ms	13 sec	1 hr	7 yrs	10^{10} yrs	10^{15} yrs
10 billion	0.02 ms	1 sec	5.4 min	245 days	10^{9} yrs	10^{14} yrs
100 billion	2 microsec	0.1 sec	32 sec	24 days	10^{8} yrs	10^{13} yrs
1 trillion	0.2 microsec	0.01 sec	3 sec	2.4 days	10^{7} yrs	10^{12} yrs
10 trillion	0.02 microsec	1 ms	0.3 sec	6 hrs	10^{6} yrs	10^{11} yrs

Source: Schneier – "Applied Cryptography – Protocol, Algorithms and Source Code in C" 2nd Edition

private key since the public key is not kept secret and is potentially available to anyone. Therefore, these systems generally require much longer key lengths to prevent brute-force attacks from succeeding in deriving the private key. For public key systems such as RSA, estimates indicate key lengths of 1,024 or 2,048 bits are required to ensure the integrity of public key systems. Although it might still be theoretically possible to crack a public key system, in practice the strength of these systems is more dependent upon how well the private key is protected and kept secret. If the private key is compromised, a new key pair must be generated immediately and all transactions using the old key pair should be terminated or made invalid.

It should be noted that the key length itself is not a guarantee of a safe system. It is the complete spectrum of security measures (organisational, procedural and technical measures) that will determine the security of a given system. For example, internet banking system designers must ensure that measures are in place to prevent eavesdropping, that secret and private cryptographic keys are stored safely and that tampering will be detected or will result in the destruction of the remaining data. Further there should be procedures in place to ensure that cryptographic keys are changed periodically and that encryption algorithms can be changed at very short notice.

Developments in cryptography are directed not only at new algorithms but also cryptoanalysis of algorithms. This is an area in which significant improvements can be expected in the next few years. Accordingly, it is critical for banks to evaluate these cryptographic measures periodically as advances in cryptoanalysis might expose weaknesses in the applied algorithms over time.

Firewalls

A firewall is essentially a barrier between computer networks to segregate and control information passing between the networks. In relation to the internet, firewalls are often the barrier between the internal network and the internet gateway. They control traffic between outside and inside a network, providing a single "choke" point where access control and auditing can be imposed. All firewalls examine the pieces or packets of data flowing into and out of a network and determine whether that piece of data should be given access inside the network. As a result, unauthorised computers outside the firewall (say the internet) are prevented from directly accessing computers inside the network. There are three main types of firewalls currently available in the market. They are packet filtering routers, proxy servers and stateful inspection firewalls.

Packet filtering routers

Packet filtering routers are the simplest form of firewalls. They are connected between the host computer of an internal network and the internet gateway. Their function is to route data out of a network and to allow only certain types of data into the network by checking the type of data and its source and destination (internet) address. If the router determines that the data is sourced from an internet address which is not on its list of acceptable or "trusted" sources, the connection would simply be refused.

The advantage of packet filtering routers is that they are generally very simple and cheap to implement. They are also fast and transparent to the users as this type of firewall requires no additional screens or log-ins. However, the disadvantage is that they generally do not provide adequate logging and alerting mechanisms to monitor traffic that crosses the firewall. If the security of the router is compromised, computers on the internal network would be wide open to external attacks. In addition, the filtering rules can be difficult to configure and poorly configured firewalls could result in security loopholes by unintentionally allowing access to an internal network.

Proxy servers

Proxy servers control incoming and outgoing network traffic by executing a specific *proxy* program for each requested connection. If a user on one company's network wants to contact a computer at another organisation via the internet, the user would actually communicate with the firewall, and the firewall would communicate with the other computer. The firewall thus serves as a proxy for all internet traffic passing through it.

The advantage of a proxy server is that it ensures that no direct connection exists between an internal network and the internet. This approach allows for a high level of control and in-depth

monitoring using logging and auditing tools. However, it doubles the amount of processing by the server which adversely affects computer performance and the ease-of-use of the firewall.

Stateful inspection firewalls

"Stateful inspection" firewalls thoroughly inspect all packets of information at the network level as in the case of proxy servers. Specifications of each packet of data, such as the user and the transportation method, the application used are all queried and verified in the inspection process. The information collected is maintained so that all future transmissions are inspected and compared to past transmissions. If both the "state" of the transmission and the "context" in which it is used deviate from normal patterns, the connection would be refused. Most of these firewalls include a real-time security alert and logs are generated for auditing purposes.

While stateful inspection is a very powerful firewall model to segregate an internal network from the internet, the performance would also decline due to the intensive inspection and verification performed.

Strength of firewalls as a security measure

The strength of a firewall is generally determined by the type of information it examines and the nature and amount of checking performed on the data before it is passed to the internal network. This means that the effectiveness of firewalls as a security tool is heavily dependent upon how the firewall is configured and the policies in place in respect of access security. Without appropriate policies and proper implementation, a firewall by itself would generally not provide adequate security to protect an institution's internal computer systems from outside attacks.

Other security measures

There are a large number of institutions that currently use the Unix operating system. This is a very powerful system suitable for the large amount of processing that occurs in a bank's daily operations. However, one drawback of Unix is the concept of a superuser account which controls all aspects of the operating system. Unauthorised access into this account could override all security measures and could potentially cripple a bank's entire computer system.

To address this problem with Unix and other similar operating systems, "Trusted Operating Systems" have been developed to segregate or *compartmentalise* functions of the superuser account so that no one person has control over all aspects of the operating system. As with other security tools however, the effectiveness of such a system is also dependent upon the surrounding security environment and the security policies implemented at the institution.

Security Policies

The importance of a comprehensive security policy

Even the most advanced technologies only provide a necessary but not sufficient condition for a secure environment. Often, the weakest aspect in a security system is due to the lack of specific security policies and enforcement of these policies in cases of security violations. Clearly, the lack of a comprehensive and rigorously enforced security policy would severely and adversely affect the effectiveness of an organisation's security system.

The objective of a security policy is to define the organisation's expectation of proper computer and network use and to define the procedures to prevent and respond to security incidents.

The development of the security policy would need to take into consideration the different requirements of the various departments and also conform to the existing policies, regulations and laws that are applicable to the institution.

A comprehensive security policy must at a minimum include the following:

- identification of assets;
- risk analysis;
- development of an acceptable use policy;
- auditing and review procedures; and
- violation response / contingency procedures.

Identifying organisational assets

In order to establish a comprehensive policy, an institution should first identify all hardware, software, data and other assets used by the institution. It should also include identification of all

users (internal, external, contract) and documentation such as programs and procedures. During this process, an institution would also need to identify all "points of entry" to its internal network available to outsiders (eg, any machine with a modem is a potential "point of entry").

Risk analysis

Risk analysis would involve identifying the assets that require protection, the likelihood of a threat and the risks involved if a breach does occur. This would enable appropriate measures to be identified and implemented to protect the assets requiring security. The analysis should cover the risk of unauthorised access to the assets, disclosure of sensitive information and the risk of the asset becoming unavailable for use by the institution (eg, due to corruption of data). For a bank, another important aspect to consider is the reputational risks as a result of a breach in security.

Acceptable use policy

A security policy must specify how users can interact with and use resources of the network. An Acceptable Use Policy (AUP) would define:

- the persons authorised to use particular resources and services;
- what constitutes proper use of resources and services;
- the resources available to internal and external users;
- the persons authorised to grant, approve or deny access to resources;
- user rights and responsibilities[1] ; and
- procedures for handling sensitive information.

An institution's security policy should specify the levels of security required of any hardware or software acquired and the various security or industry standards it should adopt. Certain hardware and software vendors submit their security products for evaluation against standards such as the Trusted Computing Security Evaluation Criteria (TCSEC) in the US which would give the product a recognised security rating. Under the TCSEC, there are six levels of security: C1, C2, B1, B2, B3 and A1. To put these ratings into perspective, a C1 rating offers essentially very little to no security. Strong "off-the-shelf" security measures would rate C2 and B1. An A1 or B3 rated system offers military grade security used by some government entities and organisations requiring very high levels of security.

Auditing and review procedures

Auditing and review procedures help to maintain the required level of security in an institution's computer system. These procedures should include reviews of user login, system usage patterns and system logs for unusual errors and procedures to ensure that only authorised programs are run on the system. The procedures would also encompass the use of monitoring tools to detect unusual activities on the system and unauthorised programs running on the system.

The results of such procedures should then be reviewed to determine any necessary changes to security tools, procedures and policies. It should be emphasised that security is inherently a dynamic process and new threats could arise requiring changes to policies and procedures and new tools to address developments in technologies.

Violation response/contingency procedures

Violation response procedures are contingency type measures that specify the actions to be taken and their priorities in case certain or all security measures fail as a result of an attack or malfunction. Such procedures would also assist institutions in taking prompt corrective action including investigation into security breaches.

At a minimum, such procedures should include the actions to be taken on discovery of a security violation. The actions taken would differ depending on whether the breach was due to an internal source or an outside intruder. However it would still require consideration of the following:

- the parties (such as management, regulators and law enforcement agencies) to be contacted and when they should be contacted; and

1 User rights and responsibilities would include the amount of resources available to users, the activities that constitute abuse, sharing of accounts, password responsibilities, consequence of disclosure of proprietary information, data privacy and policies on hacking activities.

- the persons authorised to handle any negative publicity generated as a result of the breach.

Appropriate response procedures can generally be categorised into two types: 1) protect and proceed and 2) pursue and prosecute. Under a protect and proceed approach, the primary goal is the protection and preservation of network resources and to allow resumption of normal services as soon as possible. This would involve actively interfering with the actions of the intruder to prevent further access and carrying out an immediate damage assessment and recovery. In order to achieve this, certain facilities and services of the network may have to be closed down temporarily. Such an approach, however, may not allow sufficient time for the intruder to be identified. Therefore there is a risk that the same intruder may make further attempts to access the internal network from a different path.

In a pursue and prosecute approach, the primary objective is to track down the intruder. This would require knowledgeable staff to monitor the activities of the intruder and at the same time ensure that no further damage is done. During this time, information about the activities of the intruder (including tracking of the intruder's location) can be collected and used as evidence in any subsequent prosecution. However, such an approach takes on an obvious risk that the internal systems could be damaged by the intruder.

The HKMA would expect institutions to report to it all recorded attempts at violating their security systems on a periodic basis. In cases of successful breaches, the HKMA would expect to be informed as soon as practicable but within 24 hours and discuss with the institution its steps or plans to address the incident.

Assessment of Current Security Technologies

At present, the HKMA considers that developments in internet security technologies have generally reached a point where adequate security for banking transactions is obtainable in a commercially viable manner. The use of sophisticated cryptographic techniques, firewalls and other security tools can provide security that is comparable to that offered in physical transactions. However, similar to a physical transaction, the effectiveness of such measures would be largely dependent on their proper implementation and the establishment of a set of comprehensive policies and procedures that are rigorously enforced.

However, it should be noted that this conclusion on the adequacy of security is only a temporary assessment. Continuing developments in security technologies are required to maintain the effectiveness of security measures on an ongoing basis as new threats to existing systems arise over time. Banks should accordingly be responsible for ensuring that they keep up with such developments on a continuing basis. The nature and pace of developments in information technology are such that unless banks continue to acquire state of the art technologies, their existing security measures can quickly become obsolete. This is an additional factor that should be taken into account before banks undertake to offer services through the internet.

The HKMA's Supervisory Approach

The HKMA does not wish to stand in the way of authorised institutions which seek to establish internet banking systems. It does however, require that the risks in such systems should be properly controlled.

The onus of maintaining adequate systems of control, including those in respect of internet banking, ultimately lies with the institution itself. Under the Seventh Schedule to the Banking Ordinance, one of the authorisation criteria is the requirement to maintain adequate accounting systems and adequate systems of control. This is a requirement that all authorised institutions must meet on an ongoing basis and encompasses the need to maintain systems, controls and procedures which mitigate the risk of loss of confidentiality and the risk of unauthorised access to institutions' internal computer systems. Clearly, an institution

which pays insufficient attention to these requirements could be considered as not having met the requirements of this authorisation criterion.

The current supervisory approach of the HKMA is to hold discussions with individual institutions who wish to embark on internet banking to allow them to demonstrate how they have properly addressed the security risks before starting to provide such services. Therefore, institutions intending to offer banking services electronically via an open network such as the internet should, at a minimum, consider the following:

- ensure data accessible by outsiders is encrypted using industry proven encryption techniques;
- ensure adequate measures are adopted to prevent intruders from gaining unauthorised access to the bank's internal computer systems;
- establish a set of comprehensive security policies and procedures to deal with the major aspects of security and security violations;
- monitor and report to the HKMA all security incidents on a timely basis; and
- review the adequacy of security measures (by internal and external experts) on an ongoing basis and report to the HKMA the results of such reviews periodically.

These are general security objectives which institutions intending to offer internet banking services should already have considered and taken action to address. At this present stage of development in Hong Kong, this is considered to be an appropriate regulatory response to provide a sound and secure platform for the development of internet banking. The technology and the market for such services will no doubt mature further and banking through internet might become more popular in Hong Kong in the near future. At that stage, it might be appropriate to codify the security objectives and requirements into a guideline which all institutions offering internet banking services should follow.

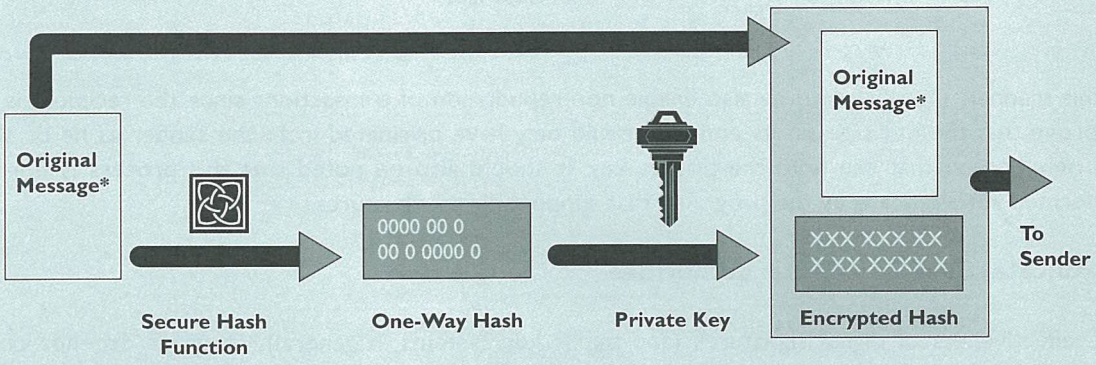
– Prepared by the Banking Development Division

Box Digital signatures, certificates, certificate authorities and public key infrastructures

Digital signatures

A digital signature is generated by first creating a separate digest or *hash* version of the message to be sent. For this purpose an algorithm will be used to scramble and shorten the message to a pre-determined length. The algorithm is formulated in such a way as to ensure that there is only one version of the hash for any given message. Common hashing algorithms include the Secured Hashing Algorithm (SHA) and Message Digest (MD) 5.

Illustration A - Generation of Digital Signatures



The sender of the message would encrypt this hash using his or her *private* key and send it together with the original message to the recipient (see Illustration A). In order to verify that the message did indeed come from the right person, the recipient would perform the following:

1) Use the sender's *public* key to decrypt the hash;

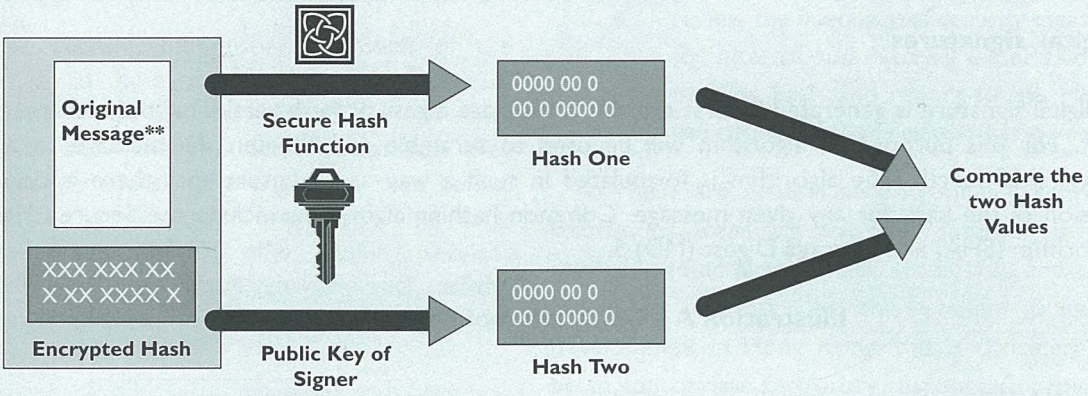
2) Generate a separate hash using the original message; and

3) Compare the two hashes.

The two hashes should be exactly the same and this would prove that the message came from the right person and that the message had not been changed in any way (see Illustration B).

* Note that for the purpose of capturing the essential features of digital signatures, it is assumed in the above that the message is transmitted in plaintext. In practice this message would also need to be encrypted.

Illustration B - Digital Signatures Verification



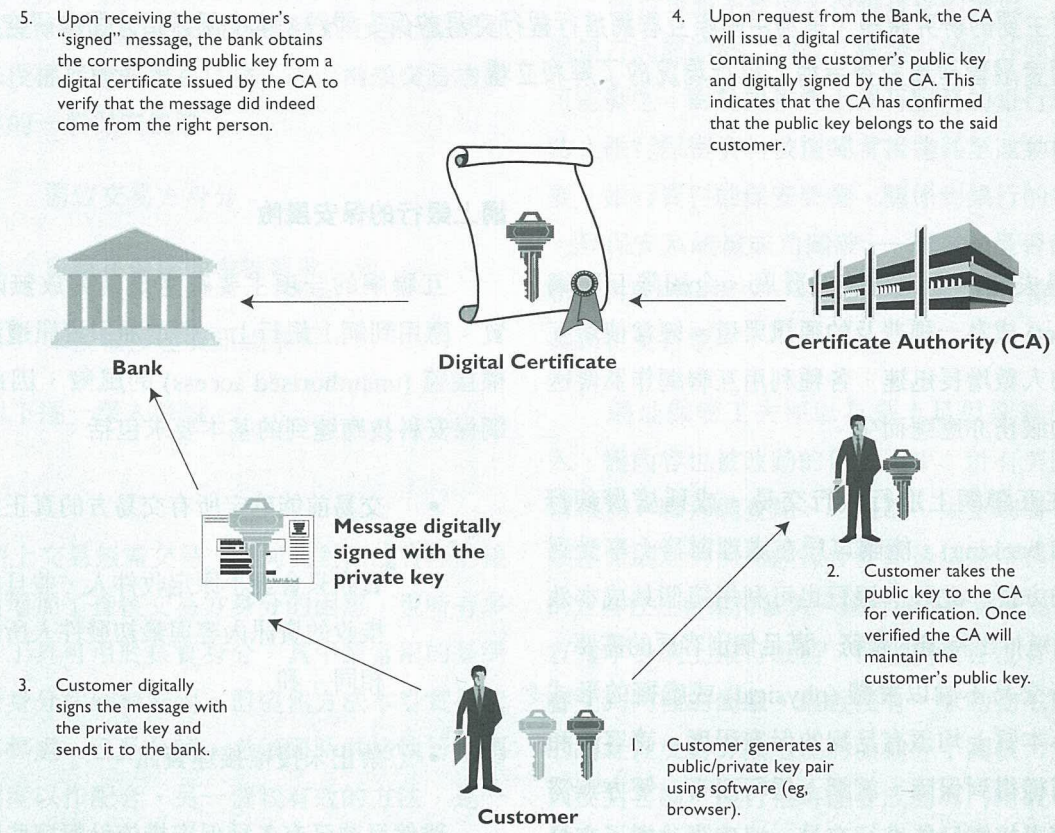
In this manner, digital signatures also enable non-repudiation of transactions since the recipient is able to prove that the message (in its entirety) could only have originated from the sender as he or she is the only person that can hold the private key. It should also be noted that this process is normally performed automatically by the programs that support digital signatures.

Certificates and certificate authorities

The effectiveness of digital signatures (and public key systems in general), however depends on the integrity of the public key and on the fact that some verification has initially been performed to associate the public key to its rightful owner. This can be achieved with the use of *digital certificates*. A digital certificate is an electronic document that binds an identity to a public key. It contains certain information such as name of the owner, validity period of the certificate, the public key and other relevant information. This set of information is verified by a *certificate authority* (CA) which digitally signs the certificate using the CA's private key to affirm the integrity of the certificate. A person who obtains a public key from a certificate issued by a CA can then rely on the fact that the CA has performed the necessary verification of the identity of the key owner and rely on this knowledge to transact using the keys. The CA thus acts as a "trusted" party and itself must maintain a very high level of security to protect its own private keys and to maintain the list of valid certificates issued. (See Illustration C on how a CA would provide this service to authenticate customers for a bank.)

** Note that for the purpose of capturing the essential features of digital signatures, it is assumed in the above that the message was transmitted in plaintext. In practice this message would be encrypted and the recipient must decrypt the message before generating a separate hash.

Illustration C - Authentication using digital certificates and CAs



Public key infrastructures

For an internet banking transaction, it is possible for a bank to act as the CA for its own customers. Banks already perform a certain amount of verification on their customers before an application is approved. However, a bank acting as a CA would need to establish strong security systems since it takes on the responsibility for maintaining the public keys of its customers. Such a scheme might be considered adequate where customers only deal with their own bank. However, this could become impractical for services across banks if different standards are adopted by individual institutions and there is a lack of inter-operability between them. Customers might also be required to hold a number of certificates associated with different banks. These factors can detract from the convenience that electronic banking aims to offer. Even outside the area of banking, this is an issue at the broader level of electronic commerce where public key systems would also be the preferred means of authentication.

One possible way of addressing this issue is to develop an effective *public key infrastructure* and to encourage the use of digital signatures in electronic banking on a broad and consistent basis by the community at large.

The aim of a public key infrastructure is to allow common standards to be adopted by all CAs. The process of cross-certification can also be further simplified by having a single entity taking on this role. Such a "root authority" will establish the standards and certify subordinate CAs that comply with its standards. A root authority would also be in a position to establish cross-certification with other recognised root authorities overseas.