**Saudi Arabian Monetary Agency**

**Banking Technology Department**

**Internet Banking Security Guidelines**

**v1.0**

**05 May 2001**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.      Introduction**                  Internet banking services and products can provide significant new opportunities for banks. It may allow banks to expand their markets for traditional deposit-taking and credit extension activities, and to offer new products and services or strengthen their competitive position in offering existing payment services. In addition, Internet banking can reduce operating costs for banking institutions.                More broadly, the continued development of Internet banking contributes to improving the efficiency of the banking and payment system and to reducing the cost of retail transactions nationally and internationally. Consumers and banks are able to increase the efficiency with which they make or receive payments, and enjoy greater convenience. Internet banking may also increase access to the financial system for consumers who have previously found access limited.                Given the degree of uncertainty about future technological and market developments in Internet banking, it is important that supervisory authorities avoid policies that hamper useful innovation and experimentation. At the same time, banks recognise that along with the benefits, Internet banking activities carry risks that must be balanced against the benefits.                The purpose of this document is to provide guidelines and considerations for banking institutions as they develop methods for identifying, assessing, managing and controlling the risks associated with Internet banking. SAMA wishes to encourage the banks to develop a risk management process rigorous and comprehensive enough to deal with all known risks, and flexible enough to accommodate changes in the type and intensity of risks associated with internet banking. The risk management process can be effective only if it is constantly evolving.                The remainder of this document is organised as follows. The next section identifies and categorises risks that banks may face in Internet banking. Section 3 presents the control objectives where risk should be minimised for a bank offering online services, while section 4 provides the risk management and control framework necessary for these objectives to be reached. Banks that decide to outsource their online service need to be aware of the risks that outsourcing endorses and the methods to manage and monitor them as described in section 5. Next, section 6 stresses the importance for managing the customer relationships. Banks must inform their customers about the risks of using their Internet service and educate them for the safest way to use it. Lastly, section 7 provides an outline of an appropriate supervisory approach which SAMA intends to adopt.    **2.      Nature of Risk Exposure Related to Internet**    Continuing advances in technology and its prominent role in commerce are leading financial institutions toward the Internet in increasing numbers. Uses of the Internet may include information-only, information transfer, or fully transactional sites on the World Wide Web (Web), or the capability to access the Internet may exist from within or outside the institution. Regardless of the use, numerous risks exist which must be addressed within the bank's risk management program. Security breaches due to some of the following factors may currently be rare, but as banks expand their role in electronic commerce they could potentially become prime targets for malicious activities.    **2.1     Distinction of Risks at Service Level**    Information Service (Low Risk)  This is the most basic form of online Internet service providing one way communication covering advertisements, promotional material, etc.  Websites are often the targets of hacking which vandalises and mutilates the original information being processed resulting in reputational harm.    Interactive Information Exchange (Medium risk)  Customers are able to communicate with the bank, make account enquiries and fill in application forms, etc.  The risk pertaining to these websites depend on whether they have any direct links to the bank’s internal network.    Transactional Service (High risk)  Allows customers to execute online transactions such as the transfer of funds, payment of bills, on-line shopping and other financial transactions, potentially including sale and purchase of securities; accordingly this is the highest risk category that requires the strongest control.    **2.2     Other Distinctions of Risk**    External Attacks  Internet-based attackers, more commonly called ‘hackers’, pose the most publicised security challenge. These individuals gain access to systems and the information they contain by exploiting flaws in the configuration of the Web server, the server’s operating system, or the actual components of the Web pages. The remote client machine (e.g. PC) is also vulnerable to direct and indirect network attacks, and physical attack.    Electronic eavesdropping is also a potential hazard, since the electronic emanations from a computer screen or cables can be detected and re-assembled into meaningful data.  Some organisations place their sensitive systems in specially screened rooms to prevent this.      Internal Attacks  Internal intrusion, or the breaching of security systems by someone within the organisation who might potentially have authorised access to hardware and software components, is another area of concern. Internal attacks are among the most serious risks that a bank faces, and can be initiated by outsiders via threats or blackmail as well as by the ambitions of insiders.  Hence, no one should have concurrent access to both production systems and backup systems, particularly data files and computer facilities as well as for operating systems, systems design and development, application, maintenance, operations, database administration, etc.    Physical security and password security are paramount in controlling illegal activity within the site manager’s own organisation. Various technology-based means exist to mitigate the risks relating to internal attacks. These also provide protection against the other generic forms of attack. Common technology solutions include intrusion detection, event logging and monitoring, and software version control.    Malicious Code  The receipt or distribution of malicious code elements (‘Trojan Horses’ or ‘viruses’) can also cause security risks and, more commonly, malicious harm to Internet-based computers and programs. Many Web sites include receipt and distribution of files and programs among the features that are offered to end-users. This is just one way in which malicious code can be distributed; other means include e-mail (with or without attachments) and network access.    Denial of Service  Denial of service and availability must also be a primary concern for site managers. As if protection from interlopers and subversive elements was not enough of a concern, system downtime resulting from power failure, wide-area communications problems, and natural disasters can also result in customer dissatisfaction and ultimate harm to the site manager’s company or group.    Mis-Service or ‘spoofing’  Mis-service is a type of attack targeting service providers which use open networks as an access channel, often overlooked by service designers and system architects. In open networks, particularly the Internet, it is sometimes possible to impersonate a legitimate user or network entity. This can be done using various techniques, such as DNS or router subversion, or by means of subverting active content in a Web browser. The end result is that legitimate users are unwittingly connected to a fake (or subverted) network entity with a view to defraud or offend. This type of attack can cause extensive reputational damage to an on-line service provider.    Negligence  Security-related negligence in the handling of sensitive data or the configuration of security systems can also be devastating. The best security systems incorrectly administered or improperly managed present increased risk potential. Inadequate policies and procedures can result in security failures or censure from regulatory agencies and auditors.    SAMA will expect banks to establish and enforce sound policies and procedures to address these risks. This document is intended to provide a framework for these to be established in a cost-effective way. The document should also provide a basis for scoping the necessary security training and awareness programmes for users and administrators alike.    **3.      Control Objectives for Internet Banking**                Security threats arising from denial of service attacks, spoofing, sniffing, hacking and other forms of illicit activity require a security policy covering the following control objectives (some of which are described in more detail in the US FDIC’s ‘Security Risks Associated with the Internet’):      Communication control    Data Confidentiality    Data and message integrity    Authentication of users and entities    Non-repudiation of transactions    Access control    Network security    Logging and audit    System availability, resilience and disaster recovery    Customer protection  **3.1     Data Confidentiality**                This refers to the protection of bank’s sensitive information and online systems and requires encryption appropriate to the type of risk present in its networks and systems by selecting encryption algorithms according to well-established international standards. Proper procedures and facilities for cryptographic key management are essential for the secure and reliable operation of all cryptographic security systems.                Unless otherwise protected, all data transfers, including electronic mail, travel openly over the Internet and can be modified or read by others. Given the volume of transmissions and the numerous paths available for data travel, it is unlikely that a particular transmission would be monitored at random. However, programs, such as "sniffer" programs, can be set up at opportune locations on a network, like Web servers (i.e., computers that provide services to other computers on the Internet), to simply look for and collect certain types of data. Data collected from such programs can include account numbers (e.g., credit cards, deposits, loans) or passwords.  More sophisticated sniffers may, for example, be looking for trading activity in certain securities in order to cheat the market.                As mentioned in *Mis-Service*, attacks using spoof Web sites can occur, whereby an attacker seeks to fool legitimate users of an on-line service to use a false Web site instead of the genuine one. Given this situation, a user’s account login information may be stolen, or the communications between the user and the false site may be relayed to the real Web site. The latter form is known as a *man-in-the-middle* attack.                Due to the design of the Internet, data privacy and confidentiality issues extend beyond data transfer and include any connected data storage systems, including network drives. Any data stored on a Web server may be susceptible to compromise if proper security precautions are not taken.    **3.2     Data and Message Integrity**                This refers to the accuracy, reliability, completeness and timeliness of information processed, stored or transmitted between the bank and its customers, with the major risk being that the banks can be accessed by anyone from anywhere at anytime.    Potentially, the open architecture of the Internet can allow those with specific knowledge and tools to alter or modify data during a transmission. Data integrity could also be compromised within the data storage system itself, both intentionally and unintentionally, if proper access controls are not maintained. Steps must be taken to ensure that all data is maintained in its original or intended form.    **3.3     Authentication**    Essential in electronic commerce is the need to verify that a particular communication, transaction, or access request is legitimate. To illustrate, computer systems on the Internet are identified by an Internet protocol (IP) address, similar to a telephone that is identified by a phone number. Through a variety of techniques, generally known as "IP spoofing" (i.e., impersonating), one computer can actually claim to be another. Likewise, user identity can be misrepresented as well. In fact, it is relatively simple to send an e-mail message that appears to have come from someone else, or even send it anonymously. Therefore, authentication controls are necessary to establish the identities of all parties to a communication.    **3.4     Non-Repudiation**    Non-repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. The former is much harder to achieve than the latter. Non-repudiation of payment instructions should be of particular concern to banks. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communications or transactions.    **3.5     Access control**                Physical attack on equipment is a serious risk.  This may just involve stealing of passwords and use on a legitimate machine which is in an unprotected area of an office. At the other extreme, it may mean a physical attack on (eg, a PIN pad) using cryogenic techniques in order to break the tamper proofing and access encryption keys stored in the device.  At both extremes, it is necessary to ensure that devices cannot be reached by intruders or by genuine staff who are intent on committing insider frauds.  The control objective here is to ensure that it is known who has access to particular machines and equipment and that this access is controlled by physical security doors, signing in and out methods etc.           Beyond physical attack, however, is virtual attack.  Bank servers connected to the Internet are vulnerable to intrusion of various kinds.  Furthermore, if unauthorised parties access the bank’s servers, this could put the bank’s customers’ systems at risk too.  The aim of network access control is to minimise these risks.  **3.6     Network security**    In general, banking systems make the assumption that networks are not secure in themselves and that therefore end to end security at the application level is necessary.  However, on an open network like the Internet, this is not possible as the client devices which may be connected via the Internet to a bank’s systems are not likely to have Hardware Security devices and software to achieve this.    At present, there is no globally accepted mechanism to get round these problems, since the Secure Electronic Transactions (SET) protocol devised by Visa, MasterCard, Microsoft and others has not been generally accepted.  The only de facto standard is Secure Sockets Layer (SSL), which is basically a line encryption mechanism which secures transactions from the browser in the client machine, to the Internet software in the host.  In recent versions of SSL, some authentication is also provided based on digital certificates.  This is probably the best achievable network security mechanism for Internet transactions at present.  It is expected that more acceptable versions of SET will be devised, and other suggestions have been made for a more rigorous approach to Internet transactions, which does not depend upon the network being secure.    **3.7     Logging and audit**                Logging of transactions and the various exchanges between computers during transactions is essential to provide a record of what data has actually passed between which machines in the course of the connection – ie the audit trail.  Best practice is to use WORM (Wrote Once Read Many times) drives to log the financial part of transactions, as these cannot easily be subverted and can readily be accessed to investigate anomalous occurrences.  The completeness and accessibility of the audit log is the key to its usefulness as a tool to detect and investigate erroneous or fraudulent activity    **3.8     System Availability**                The users of Internet banking services expect to be able to access the online systems 24 hours every day of the year. Among the considerations associated with system availability are capacity, performance monitoring, redundancy, and business resumption. Local banks and their suppliers who provide Internet banking products and services need to ensure they have the capacity in terms of hardware and software to consistently deliver a high level of service.    Key areas to which providers of on-line services should attend are resilient design, data backup and recovery, fail-over and contingency against denial-of-service attacks.                In addition, performance monitoring techniques can provide management with information such as the volume of traffic, the duration of transactions, and the amount of time customers must wait for service. Monitoring capacity, downtime, and performance on a regular basis will help management assure a high level of availability for their Internet banking system. It is also important to evaluate network vulnerabilities to prevent outages due to component failures. An entire network can become inoperable when a single hardware component or software module malfunctions. Hence national banks and their suppliers should deploy contingency hardware in critical areas or have the ability to switch to alternate processing locations.    **3.9     Customer Protection**    Limiting access to information to only those authorised to receive it and transmitting data in a way that ensures privacy are the first steps to successful Internet security. The most common method of restricting data access on the Internet is User ID and Password requirements. It is now vital to protect against sophisticated programs that can replicate the login efforts of a user, utilising a pattern of codes designed to uncover the authentic User ID and Password assigned to a specific user. This threat is also caused by the possibility of spoof Web sites. Web-based financial applications must use measures like limiting the number of incorrect logins and the tracking of unsuccessful access attempts in order to protect the confidentiality of the User IDs and Passwords themselves. There are many different approaches which can be used to thwart successful attacks, including alerting users to attempted attack by advising the time and date of the last successful log-on, the number of unsuccessful log-on attempts since the last successful log-on, and the details of the last user transaction.    From a procedural standpoint, it is also vital that financial information providers create and implement secure methods for producing and issuing customer codes. User ID and Password controls must become part of the documented, enforced, and audited procedures of every financial institution that maintains more than a marketing presence on the Internet. Separation of duties and dual control within the operations area that maintains user access information and/or the Web site itself must be maintained as rigorously as they are in the cash vault or other key areas of the financial institution. The most secure technology, poorly managed, will prove ineffective.    **3.10   Conclusion**    SAMA takes the view that the banks should address each of these control objectives in order to ensure an acceptable level of security in Internet banking and payment systems. In the next section, a control framework is suggested which is intended to provide guidelines for the banks in establishing sound Internet banking security practice.    **4.      A Risk Management and Control Framework**                  Having made an assessment of risks and defined the control objectives, bank management should take steps such as the following to manage and control risks.      Develop and implement security policies    Agree on and implement administrative and procedural control methods    Implement and maintain technical control methods, which will be embodied in the security architecture, applications, policies and procedures.    Cryptographic techniques and communications security    Best practice in internet payment security, using cryptographic techniques    Management of cryptographic security systems    Firewalls    Infrastructure (host system) security methods    Control of interfaces between the bank site and the web    Maintain and regularly test a recovery and business continuity plan    Manage any outsourced processes in a secure fashion (discussed in section 5)    Manage customer relationships taking security into account (discussed in section 6)    A basic list of control measures is provided in Appendix 1.    **4.1     Security Policies**                Effective security relies on the development and implementation of adequate security policies and security measures for processes within the bank, and for communication between the bank and external parties. Security policies can limit the risk of internal and external attacks on Internet banking systems, as well as the reputational risk arising from security breaches.                A security policy states management’s intentions to support information security and provides an explanation of the bank’s security organisation. It also establishes guidelines that define the bank’s security risk tolerance. These include administrative guidelines, user guidelines and contingency procedures. The policy may define responsibilities for designing, implementing, and enforcing information security measures, and it may establish procedures to evaluate policy compliance, enforce disciplinary issues, and report security violations.      **4.2     Administrative and procedural - HR and business controls**                Administrative controls are formalised standards, rules, procedures, and control disciplines to ensure that the organisation’s general and application controls are properly executed and enforced. The most important administrative controls are:      segregation of functions    written policies and procedures    supervision of personnel    ***Segregation of functions*** means that job functions should be designed to minimise the risk of errors, avoiding a single point of failure or fraudulent manipulation of the organisation’s assets. The individuals responsible for operating systems should not be the same ones who can initiate transactions that change the assets held in these systems. A typical arrangement is to have the organisation’s information systems department responsible for data and program files and end users responsible for initiating transactions such as payments or checks. These controls are particularly important around the management of Internet payment systems.    Similar principles apply to the process of cryptographic key management where, for example, it is common practice to split cryptographic keys used to secure certain security processes, such that two or more personnel are required to co-operate to use the key. This is generically referred to as a *delegate scheme*.  Such control is particularly important when root keys for cryptographic systems are changed, since this creates an opportunity for unauthorised access to entire systems.    ***Written policies and procedures*** establish formal standards for controlling information system operations. Procedures must be formalised in writing and authorised by the appropriate level of management. Accountabilities and responsibilities must be clearly specified.    Some of the simplest and most effective of these concern control of access to sensitive technology areas, such as rooms used for Certification Authority systems (described below),  In such areas, for example, only certified software should be taken in, all operational systems should be compiled from certified source code within the controlled environment and no personal PC’s, laptops, briefcases etc should be allowed.  These simple measures, properly enforced, eliminate the risk of many kinds of technical attack.      ***Supervision of personnel*** involved in control procedures ensures that the controls for an information system are performing as intended. Without adequate supervision, the best designed set of controls may be bypassed, short-circuited, or neglected. Compliance checks for Internet banking systems and procedures must be conducted regularly.      **4.3     Technical – Control Methods**  **4.3.1**       **Cryptographic techniques and communications security**                Cryptography is the science of encoding messages so their content can only be understood by the intended recipient, or generated by the intended originator. Encryption is used to protect the transmission of sensitive digital data across computer networks or, increasingly, to keep sensitive computer files private while they remain stored on a computer. The messages are changed from readable to unreadable and back again using complex mathematical algorithms with digital ‘keys’. There are two basic encryption techniques:      Symmetric algorithm (or secret key)    Asymmetric algorithm (or public key).                In ***symmetric algorithm systems***, the sender and receiver of a message each use the same secret key: the sender uses it to encrypt a message, and the receiver uses it to decrypt this message. The most important aspect of symmetric key encryption is that encoding and decoding can be performed very quickly. Furthermore, symmetric keys can be generated with great ease compared to asymmetric keys.                Encrypted messages can also be used to meet another of the control objectives – message integrity.  Modifications made to encrypted messages cause unpredictable results to the subsequent process of decrypting the message. It is possible to implement a scheme to ensure that any attempt to make an illicit modification to an encrypted message is detected. To achieve this, the original message is passed through a hash function to create a message digest, then the digest is encrypted using a symmetric algorithm and a secret key known only to the message sender and the intended recipients. The resulting data is a Message Authentication Code (MAC) which is sent together with the encrypted message. The recipient decrypts the message and regenerates the MAC; if it does not match the MAC received from the originator, the message is known to be corrupt.                Secret key encryption is a simple and straightforward method, but it has an inherent vulnerability in that both parties must possess the same key. In other words, the same key has to be communicated between both parties without anyone else coming into possession of it, either inadvertently or through sinister intent. If these parties are proximate, the chance of compromise is not a large one. However, if the parties are in separate physical locations, which is most often the case, they must rely on a third party, such as a telecommunications system, to distribute the secret key between both parties without anyone else coming into possession of it, or distribute the secret keys themselves. It should be noted that symmetric algorithm cryptography, in view of the common shared secret keys between originator and recipient, cannot be used to implement non-repudiation schemes.    In ***asymmetric algorithm systems***, two keys are used. One key is kept secret, and therefore is referred to as the ‘private key’. The other key is made widely available to anyone who wants it, and is referred to as the ‘public key’. The private and public keys are mathematically related so that information encrypted with the private key can only be decrypted by the corresponding public key and *vice versa*. The private key, regardless of the key system utilised, is specific to a party or computer system. Therefore, the sender of a message can be authenticated as the private key holder by anyone who decrypts the message with a public key. This property permits non-repudiation schemes to be implemented.    Importantly, it is mathematically infeasible for the holder of a public key to use it to calculate what the private key is. The keys can be stored either on a computer or on a physically separate medium such as a smart card. This is particularly important if non-repudiation is to be proved at a user level. Public key cryptography is therefore a powerful tool for maintaining confidentiality of information. Its major drawback is speed.    Public key cryptography can thus be used not only to provide data confidentiality and message integrity but also authentication of users and non-repudiation. A further step in authentication is the use of ***digital signatures***, which can be achieved using public key cryptography. Digital signatures authenticate the identity of a sender, through the uniqueness of the private cryptographic key. In addition, every digital signature is different because it is derived from the content of the message itself. The combination of identity authentication and unique signatures results in a transmission that cannot be repudiated.    The process for generation of asymmetric algorithm key pairs is considerably more complex than that for generating symmetric algorithm cryptographic keys and thus requires considerably more  processing power or more time. In order to combine the benefits of low processing speed  for symmetric algorithm cryptography, with the benefit of key distribution and non-repudiation for asymmetric algorithm cryptography, it is often desirable to create a hybrid cryptosystem. In such a scheme, public key cryptography will be used to authenticate parties, to distribute keys and to provide non-repudiation, whilst private key cryptography will be used to provide efficient message integrity and confidentiality.    Digital signatures can be applied to any data transmission, including e-mail. To generate a digital signature, the original, unencrypted message is run through a hash function, as described above for MACing, to generate a message digest. The message digest is then encrypted with a private key, and sent along with the message. The recipient receives both the message and the encrypted message digest. The recipient decrypts the message digest using the known public key, and then runs the message through the hash function again. If the resulting message digest matches the encrypted one sent with the message, the message has not been altered and data integrity is verified. Because the message digest was encrypted with a private key, the sender can be identified and bound to the specific message. The digital signature cannot be reused, because it is unique to the message.    For non-repudiation, it is also necessary to ensure that a message is timestamped to indicate its temporal validity. In other words, to detect an attempt at replaying a message, delaying a message or modifying the order in which messages have been sent. In the above example, data privacy and confidentiality could also be achieved by encrypting the message itself. Hence all the communication control objectives are met. The strength and security of a digital signature system, however, are determined by its implementation, and the management of the cryptographic keys.                Regardless of the key system utilised, physical controls must exist to protect the confidentiality and access to the private (or secret) keys and the integrity of *all* keys. In addition, the key itself must be strong enough for the intended application. The strength of the key is determined by its length.  The longer the key, the harder it is for high-speed computers to break the code.  The appropriate encryption key may vary depending on how sensitive the transmitted or stored data is, with stronger keys utilised for highly confidential or sensitive data. Stronger encryption may also be necessary to protect data that is in an open environment, such as on a Web server, for long time periods.  Currently, the keys normally used for asymmetric encryption processes with the most popular algorithm (RSA) are 1024 bits long.    **Management of keys** for Public Key systems and the proof of the ownership of Public Keys demands the existence of trusted authorities who can issue reliable digital certificates (Certification Authorities or CA’s). CA systems should be housed securely and not normally be connected to networks.    A  trusted authority need not necessarily be a third party, depending upon the relationship between the communicating parties. A Certification Authority can become the hub of a Public Key Infrastructure (PKI) whose participants can be confident that their mutual use of the Public Key system is fully reliable.  SAMA will be establishing a Public Key Infrastructure (PKI) for the Saudi banking industry and expects that the banks will implement secure payment methods using the SAMA PKI framework. The security technique to be used (SSL, SET, etc.) is currently under discussion.    **4.3.2   Secure payment on the Web**    Netscape's ***Secure Sockets Layer (SSL)*** protocol is currently the most widely used method for performing secure transactions on the Web and is supported by most Web servers and browsers including Netscape Navigator and Microsoft Internet Explorer. The Secure Sockets Layer (SSL) protocol provides several features that make it particularly attractive for use in some e-commerce transactions. However, software-only security solutions, such as SSL, cannot provide robust and complete security at the Browser. As such, they are only part of a set of security mechanisms for securing client-server transactions over a public network.  If SSL is used in isolation, the security architectures will be incomplete, and hence susceptible to subversion at the client or via exploitation of security vulnerabilities in active content via spoof Web sites.                Essentially, SSL is secret-key encryption nested within public-key encryption, authenticated through the use of certificates. The reason that both secret-key and public-key encryption methods are used is because of the relatively slow speed of public-key encryption compared to secret-key encryption. Initially, the client (the web browser in an Internet payment transaction) generates a private encryption key which it encrypts using the public certificate of the server with which it is to establish a secure session. The client sends this encrypted key to the server, which then recovers the key, this being used only for this transaction. This is referred to as a session key. Then, for the rest of the transaction, the client and the server can use the session key for private-key encryption of messages exchanged in either direction between the client and server.                Additionally, message digests of each message exchanged between client and server are also encrypted using the private key to create MACs, which are appended to each respective message. These are verified by the recipient to ensure message integrity.  This process is used to protect eg credit card details and customer data for the payment element of the transaction.    SET is the ***Secure Electronic Transaction*** protocol developed by Visa and MasterCard specifically for enabling secure credit card transactions on the Internet. It uses digital certificates to ensure the identities of all parties involved in a purchase and encrypts credit card information before sending it across the Internet.    The SET model has four types of participant; the Card Issuer (Brand Owner), the Customer, the Merchant and the Merchant Acquirer. In a typical SET transaction, there is information that is private between the customer and the merchant (such as the items being ordered) and other information that is private between the customer and the bank (such as the customer's credit card number). SET allows both kinds of private information to be included in a single, digitally signed transaction. Information intended for the bank is encrypted using the bank's public key whilst information for the merchant is encrypted with the merchant's public key. This means that the merchant has no access to the credit card details and thus a source of fraud is eliminated. In addition to this encryption, both sets of information are digitally signed. Finally these two signatures are combined to produce one signature that covers the whole transaction.    Like SSL, SET allows for the merchant's identity to be authenticated via digital certificates. However, SET also allows for the merchant to request users authenticate themselves through digital certificates. This makes it much more difficult for someone to use a stolen credit card.    There are many pilot schemes running using the SET protocol but mainstream adoption has been slower than predicted. The main reasons behind this are the growing acceptance of SSL for secure credit card transactions and the complexity and cost of the SET system.   There are now simpler versions of SET being trialled including a zoned version called 3D SET which does not require all the participants to be linked by a single set of certificates.  It is not yet clear whether this will receive general acceptance.    SAMA intends to keep an active watch on this area and make recommendations when the techniques have reached the appropriate level of maturity.    **4.3.3   Management of Cryptographic Security Systems**                All operational cryptographic security systems require security management in order to ensure that the system works efficiently and securely, both in normal day-to-day operation and in the event of exceptional circumstances (such as revocation or recovery). This section applies equally to cryptographic keys and to digital certificates (unless otherwise specified).     Key generation    The process of generating cryptographic keys requires at least that a (pseudo) random number generator facility is available for creating candidate values for keys. Further processing may be required, for example, when public-private key pairs are to be generated. Keys may be generated in advance, however any such keys would need to be securely stored (see *Key archiving*). All robust implementations of most popular algorithms require that “weak keys” be eliminated. These are keys, which cause the algorithm to operate ineffectively.     Key distribution    The process of key distribution requires all distributed keys to be transmitted in such a way as to ensure integrity, and that secret (or private) keys are distributed in a secure manner.  This also applies to cryptographic certificates. Some architectures require the use of hardware devices to transfer secret cryptographic keys (such as smart cards) or the use of key-splitting between individuals. Some architectures employ the use of special algorithms to permit mutual agreement of cryptographic keys in a secure manner between communicating parties over an insecure channel.     Key archiving    The archiving of cryptographic keys requires a facility, which can provide both physical and logical security. Typically, this might be implemented with the use of a Hardware Security Module (HSM).     Root certificate distribution    Root certificates need to be reliably distributed throughout their relevant domains within a PKI architecture. Within a PKI architecture, each entity which relies upon cryptographic certificates will require a copy of the root CA public key(s).  SAMA’s PKI approach will include secure methods for all the necessary processes.     Token management    Secure tokens need to be managed securely. Typical secure tokens are smart cards, which need to be pre-personalised and distributed in a secure manner. An associated task is token PIN management (see below) and token revocation.     PIN mailing    User passwords (or PINs) are an essential mechanism for authenticating users. The PINs associated with secure tokens need to be securely distributed to their respective users. The most popular way of achieving this within the banking sector is by means of PIN mailing, carried out via an integrated secure procedure.     User registration    In a PKI, the secure registration of users is of paramount importance. All security hinges on the end user actually being positively authenticated. A great deal of care needs to be taken to ensure that the technology and procedures relating to user registration are secure.     Certification    Certification of cryptographic keys (or other security attributes) is a fundamental process within a PKI. The technology and procedures relating to this need to be secure. Core policy relating to the proper operation of a PKI is the Certificate Policy, in conjunction with the Certificate Practice Statement. The content of these documents needs to be carefully constructed and adhered to.     Certificate revocation    Any certificate issued within a PKI has a finite life, and may be revoked before that time. The process of certificate revocation is a fundamental process within the secure operation of a PKI, and requires careful attention to technical design and related policy and procedure.     User account recovery    From time-to-time, users need to have their accounts recovered, normally in the event of their forgetting their passwords or PINs, or in the event of their losing their tokens. Naturally, the process and technology securing user account recovery need to be robust.     User data recovery    From time-to-time, users need to have their data recovered, normally in the event of their forgetting their passwords or PINs, or in the event of their losing their tokens. Naturally, the process and technology securing user data recovery need to be robust.     Delegate schemes    In order to control access to high-level security functions, such as root key operations or user data/account recovery, it is prudent to require the co-operation of more than one security administrator. This is normally achieved by means of a *n-of-m* delegate scheme, whereby *n* administrators need to co-operate from a larger group of *m* administrators. This is specified in policy and procedure, and implemented using appropriate technology.    **4.3.4   Firewalls**                A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that exists to block traffic, and the other that exists to permit traffic. The most important thing to recognise about a firewall is that it implements an access control policy.                Firewalls operate at various sensitivity and protection level. Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems.                Generally, firewalls are configured to protect against unauthenticated interactive logins from the ‘outside’ world. This, more than anything, helps prevent vandals from logging into machines on the bank’s network. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside. Firewalls are designed to protect a bank’s Internet service against many types of network-borne attack, however they cannot be relied upon alone to provide defence against malicious code attacks or denial-of-service attacks.                Firewalls are also play an important role in providing a single ‘choke point’ where security and audit can be imposed. Unlike a situation where someone dialling in with a modem is attacking a computer system, the firewall can act as an effective ‘phone tap' and tracing tool. Lastly, firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc.    **4.3.5   Host system security methods**                Banks can develop and implement their own preventive measures, but further measures are needed throughout the network. E-security must also become a top priority for infrastructure providers to slow down or prevent attacks from spreading - before they get out of control. Infrastructure providers include web site and application hosts, developers of the servers and routers that deliver messages over the Internet, and Internet service providers (ISPs), the gateways to the web.    ISPs should have installed virus-scanning technology that would prevent infected files from even reaching their subscribers, a feature that is being well received in the marketplace. According to recent studies, anti-virus technology is the leading choice of features for which end users would be willing to pay an additional subscriber fee.    There is a wide variety of other types of security application which, may be necessary to provide a complete, robust security architecture, including intrusion detection, Virtual Private Networks (VPN)s, secure remote access and client firewalls.    A major concern for banks implementing Internet banking and payment systems is the risk that internal or external third parties could access customers’ data held on the host system. This is a major concern where SSL rather than SET methods of secure transmission are used, because native SSL, being merely a line encryption method, does not secure data all the way back to the host (however, third party applications can permit the creation of *persistent encryption* through SSL hosts). Banks should be aware of this security gap and take measures to protect all customer data.    **4.3.6**       **Control of interfaces between the bank site and the web**                This section provides an overview of security risks associated with Internet portals and potential technological mitigation available for those risks.  Whether a bank’s site is accessible directly by users from their browsers or via other web portals, these issues need to be considered.                Various candidate solutions for the secure communication between Internet portals and their users have been suggested on the basis that they aim to provide authenticity, confidentially, integrity and non-repudiation., The candidate solutions are compared below against these criteria. Each solution is examined in its own right, against its alternative and also against the “username & password only” option.    Popular options are:-    ·        Standard Web server and client browser, secured using standard SSL (HTTPS channel)– the “SSL only” option, defined to include also a username and password login  ·        Standard client certified web (HTTPS) plus physical token – the “SSL + token” option  ·        VPN Secure client with physical token and application on CD – the “VPN + token + CD-ROM” option    This section explores technical options to mitigate risks in these options, in the context of the particular concerns of the financial sector. These being:-    ·        Minimising the impact on customers  ·        Deployment, support and manageability of solution  ·        Cost of solution  ·        Time to market of solution  ·        Merchant reaction to, and ease of use of solution    The main risks which an acceptable solution must protect against are:    ·        Weak authentication to the host allowing an unauthorised individual to authenticate as a valid user  ·        Disclosure of information while in transit between the host and the user  ·        Masquerade attack on the host server where a user is fooled into logging into a false host system (site impersonation)  ·        Relay attack on users of the host system where data is intercepted in transit between user and host (man-in-the-middle)  ·        Disclosure of data stored on remote workstation during or after a session  ·        Trojan Horse attack on the remote workstation where the client application is subverted  ·        Weak audit trails that make user accountability difficult    There are additional risks associated with access from Internet portals, e.g.:-    ·        Escalation of privilege within the host applications via authorised channels  ·        Escalation of privilege within the host applications by modification of the Access Control mechanisms  ·        Accessing information directly via a penetration of the data repository  ·        Accessing information by subversion of any custom code used for user and privilege management    These are not generally within the scope of this section, however certain parts of the solutions proposed will have the effect of mitigating these risks to a degree by virtue of their implementation or as product of the components used.    In summary terms, these options and their mitigating effects on the associated risks are as follows:-     |  |  |  |  | | --- | --- | --- | --- | | **Risk** | **SSL Only** | **SSL + Token** | **VPN + Token + CD-ROM** | | Weak authentication | DD | CC | CC | | Disclosure in transit | DD | CC | CC | | Masquerade | DD | DC | CC | | Man in the Middle | DD | C | CC | | Network access to data stored on remote workstation during active session | DD | DD | DC | | Access to residual data stored on remote workstations | DD | DD | DC | | Subversion of client application | DD | DD | C | | Weak audit trails | DD | DC | DC |     DD = No mitigation  D    = Poor mitigation  DC = Some mitigation but can be compromised under determined effort  C    = Acceptable mitigation  CC = Good mitigation    The analysis underlying this table is provided in Appendix 2.              In summary, it is clear that SSL alone does not provide the bank with confidence that its Internet service is secure.  The VPN option requires additional software and hardware at the remote workstation. The VPN software is tightly integrated with the remote workstation and server and would require installation of software drivers and might require hardware readers.  This is possible for closed user groups, but is not feasible for allowing access to the general population of potential customers.  It is probable that methods will evolve towards treating the bank’s group of Internet banking customers as a closed user group on a VPN, but this is not feasible in the short term.              Hence, SAMA would prefer to see Internet banking secured using SSL plus a token.  However, it is recognised that global best practice has not reached this point yet and that it may not be feasible in the short term to implement tokens.  The advent of EMV multi-application smart cards may provide the opportunity to implement this kind of approach, as the token could be contained on the EMV card.  In the meantime, although SSL does not overcome the risks discussed in this section it does provide advantages for payment transactions as discussed above, and should therefore be deployed by all banks introducing Internet services.    **4.4     Recovery and Business Continuity**              Recovery and business continuity procedures are important for all banking operations, but take on a new aspect where online customer access is provided and expected.    **4.4.1   Business continuity plans**              An effective contingency plan must document 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 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.    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:    protect and proceed and    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 take 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 intruder could damage the internal systems.    **4.4.2   Cryptographic business continuity planning**  The operation of a cryptographic security system within a business system requires special facilities to support business continuity and disaster recovery.  The main areas for attention are listed here.  For definitions of terms, refer to Section 4.3.3 (Cryptographic Security Management).      Key architecture     A cryptographic security system should be carefully designed to accurately reflect the trust relationship and security roles laid down in relevant security policy.  That is, who can rely on whom and under what conditions.      Key recovery    It is essential, if cryptography is used to secure messages or data (beyond a point-to-point secure session), that a reliable and secure mechanism exists to recover the cryptographic keys used to secure the messages.      PKI resilience    Given that a PKI will typically be supporting production IT systems in a business-critical situation, the PKI needs to be designed and operated in a manner which affords sufficient resilience. Particular care needs to be given to availability, recoverability, scalability and quality-of-service.      HSM recovery    The use of Hardware Security Modules in a cryptographic security system requires careful planning to ensure that the respective master keys are securely managed and that disaster recovery is properly provided for. HSM specification and master key management is also a crucial area of attention in designing resilience (dynamic load balancing and fault tolerance) through redundant infrastructure.      User data recovery    It is essential, if cryptography is used to secure messages or data (beyond a point-to-point secure session), that a reliable and secure mechanism exists to recover user data.      User account recovery    It is essential, if cryptography is used to secure access to user accounts (e.g. by means of a cryptographic token), that a reliable and secure mechanism exists to recover the cryptographic keys used to secure the account access.      User token recovery    It is essential, if cryptography is used to secure access to user accounts using a cryptographic token (whether hardware or software), that a reliable and secure mechanism exists to recover the tokens used to secure the account access      Delegate schemes    In order to control access to high-level security functions, such as root key operations or user data/account recovery, it is prudent to require the co-operation of more than one security administrator in a recovery situation       Mass certificate revocation and replacement    A core contingency capability in support of business continuity and disaster recovery is the ability to perform mass revocation of cryptographic certificates and replacement of those certificates. Given a disaster whereby, for example, a root key might have been compromised, the administrators of a PKI must have the option to revoke certificates en masse and provide replacements with a minimal disruption to business continuity.      **5.      Managing Outsourced Processes**                  A growing trend in the industry is for banks to focus strategically on core competencies and rely on external parties specialising in activities outside the bank’s expertise. While these arrangements may offer benefits such as cost-reduction and economies of scale, outsourcing does not relieve the bank of the ultimate responsibility for controlling risks and liabilities that affect its operations.    **5.1     Risks in Outsourcing Internet Banking**                Institutions deciding on outsourcing their Internet banking service should be aware of general and specific risks. General risks include the risk that the vendor will not deliver the service as agreed, will deliver less than expected, or will deliver the service late. More specific risks include the following:      If the vendor fails to meet standards, information systems services may degrade.    If the bank does not manage its vendor, the bank may lose control of the direction and quality of its Internet banking system.    Without vendor support, the bank’s ability to introduce innovative new services or upgrade current services is extremely limited.    If the bank’s information systems personnel feel that they cannot affect outsourced systems, their productivity and morale may decline.    If the vendor does not meet standards or work well with users and information systems personnel, client efficiency and productivity will deteriorate.    It becomes more difficult to keep the organisation’s business private (must be shared with outsourcer who does not have a vested interest in keeping it confidential)    The vendor could use the business knowledge they gain to become a competitor of the client or to use it for other clients as well.                If the outsourcer does not do the work according to the norms and original agreements, there is the necessity to hire another vendor to do exactly the same work. This results in reduction of productivity and could cause the bank’s reputation to be harmed.                Banks that outsource to off-shore programming companies may find that differences in culture, language, laws, business practices and hours of business may lead to communication problems that are difficult to manage, especially in a fast-paced environment.                There are several risk areas that banks need to consider in relation to prospective outsourcing of their security functions, processes or infrastructure. Such risk areas include management risk, security risk, marketing/brand risk, compliance risk, data protection risk, reputation risk and financial risk.  More details are provided in Appendix 3.      **5.2     Control of Outsourcing and Monitoring of Arrangements**                The outsourcing risk factors mentioned above have indirect influence on the availability, integrity, confidentiality and vulnerability of information and its infrastructure. Consequently, banks should adopt policies to limit risks arising from reliance on outside service providers. For example, bank management should monitor the operational and financial performance of their service providers; ensure that contractual relations between parties, as well as the expectations and obligations of each party, are clearly understood and are defined in written, enforceable contracts; and maintain a contingency arrangement to change service providers in a prompt manner, if necessary.                In addition, control of outsourced functions and operations can be maintained by closely scrutinising the vendor’s reputation, investigating the quality of services provided by the vendor to other clients, incorporating measurable performance criteria in the contract, and devising risk- and reward-sharing plans with the vendor.                Security of the bank’s sensitive information is of critical importance. The outsourcing arrangement may require the bank to share sensitive data with service providers. Bank management should evaluate the ability of the service provider to maintain the same level of security as though the activities were conducted in-house, through the review of service providers' policies and procedures aimed at protecting sensitive data. Additionally, supervisors may wish to have the right to independently assess, when necessary, the competence and the operational and financial performance of the service providers.                Vendors have contracts with different clients, so sometimes experiences received during co-operation with one vendor could be useful to develop co-operation with another, although the first client could treat it as disclosure of the confidential information. Typically, clients do not have the opportunity to bring previous personal experience to the negotiating table, while the outsourcer has negotiated numerous contracts. Therefore, it is essential to hire an adviser  with experience in information technology and financial law.                The establishment of a control mechanism can assist bank management in improving the quality and production of their operation. There is plenty of advice in the outsourcing literature to build in contract variation clauses, agree on annual reviews, sign short-term contracts, and so on - if the vendors will agree. Short-term contracts may attract cost premiums, and contract variation clauses may not foresee all the uncertainties.                Furthermore, uncertainty affects all IS operations in terms of introduction of new technology, the intensity of IT demand, change in organisational environment and change of market conditions Neither user nor outsourcer can know about future possible cost savings or foresee technological discontinuities. In practice, companies tend to underestimate the management costs and set-up costs of outsourcing, including redeployment costs, relocation costs, and longer-than-expected hand-off or parallel running costs. Thus IT contracts should specify a process of conflict resolution and problem solution for the inevitable uncertainties.      **6.      Managing Customer Relationships**    Banks offering online services face the challenges of:      Identifying and addressing consumer concerns about transacting online    Identifying areas of exposure or vulnerability due to insufficient disclosures    Building and sustaining the confidence of customers    Customers’ inexperience    Persuading customers to accept the impact of secure access technologies    Carrying the cost of secure access technologies      Banks can overcome the above challenges by implementing the following two strategies:      Disclosing risks to customers    Educating customers      **6.1     Risk Disclosure to Customers**                To realise the full potential of the Internet, banks have to establish a relationship of communicating with their customers about online security and privacy. When customers are unsure of a bank’s online policies, they are more likely to abandon a transaction or provide false, inaccurate, or incomplete information.                Banks should provide clear information to customers about the risk and benefits of using Internet banking. Accordingly, they should publish their customer privacy and security policy, dispute handling, reporting and resolution procedures, etc.                Banks must publish online a user agreement that outlines the terms and conditions of using Internet banking, including the access requirements, fees and charges, security issues, terms and conditions, etc. The bank should clearly describe the features of its Internet banking service, such as availability of fund transfers, account balance, and the ability to make transactions.                Banks must try to communicate to their customers the belief that their online service meets all the security standards. Customers need to know if the bank provides continuous monitoring and auditing of all transactions originating from or outbound to the internet, if it operates within all the rules and regulations of the banking and financial industry for internet commerce, and if the bank is committed to producing the safest operating environment possible. Comprehensive security guidelines must be published.                  Banks have to state the level of encryption used by their system (typically 128-bit Encryption for SSL) and other security controls such as firewalls, explaining their use to the customers.  They should also explain to users what benefits these technical features provide. In so doing, banks should take great care not to imply levels of security which are not achievable in practice, or to lull users into a false sense of security. Security is always as strong as the weakest link; no attacker would reasonably attempt a brute-force attack on the cryptographic keys for 128-bit SSL, when there are several means of successfully attacking the SSL application and architecture by exploiting inherent weaknesses.    Banking institutions that understand the concerns of their consumers -particularly as they relate to security and privacy - and communicate their policies openly will make significant progress toward building lasting online customer relationships, managing the risks of the new economy, and minimising the costs related to customer misunderstandings.      **6.2     Customer Education**                As banks open up their systems and launch Internet banking, they invariably increase their risk and vulnerability. Consequently, banks are seeing the heightened imperative of building confidence into their digital business systems and relationships.                The very open, connected nature of e-business calls for an increased amount of trust among customers, and Internet banking service providers. Trust that a customer's confidential data will remain confidential. Trust that the information supplied to others in a network is correct and of the highest integrity. And trust that systems will be up and running-available 24/7, as needed in Internet time. A way to build this trust is by educating the customers. Banking institutions should educate customers in the following areas:      how to use new products and services. Banks should provide sufficient information for their products and services and instructions for their use, e.g. with a demonstration.    how to avoid security breaches in their transactions.    technical matters and the value of technical features, e.g. type of Internet browser, computer requirements, etc.    how to react in problematic situations, e.g. in the case of a fraud.    how to select and use a password. Example guidelines might include:    The customer’s password should be at least a certain number of characters long (preferably 6-8). It can be a combination of letters and/or numbers.    The customer should not use personal information that is easy to guess, such as address, birthdays or a family member's birthday, driver's license number, etc.    Customers should memorise their password. They should not write it down or reveal it to anyone.    Change the password often (it can be done online within the Internet banking system).      **7. Central Bank Supervisory Approach**                SAMA does not wish to discourage the banks from establishing Internet banking systems. However, it is required that the risks in such systems should be properly controlled and monitored. The onus of maintaining adequate systems of control, including those in respect of Internet banking, ultimately lies with the institution itself.                SAMA’s supervisory approach involves:      holding 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    inclusion of specific Internet banking issues in SAMA’s regular off-site and on-site bank examination processes    encouraging Internal Audit review of Internet banking facilities, systems and processes    Therefore, institutions intending to offer banking services electronically via an open network such as the Internet should, as a minimum:    ensure data accessible by outsiders is encrypted using industry proven encryption techniques. Noting that widely-used may not be the same as highly secure. Minimum 128 bit keys should be used for SSL implementations      take particular care to ensure the physical and electronic security of root keys and any Certification Authority systems used      ensure adequate measures are adopted to prevent intruders from gaining unauthorised access to the bank’s internal computer systems, including physical controls and the risk of electronic eavesdropping      establish a set of comprehensive security policies and procedures to deal with the major aspects of security and security violations    monitor and report to SAMA all security incidents on a timely basis      review the adequacy of security measures (by internal and external experts) on an ongoing basis and report to SAMA 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, 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. There may be legal changes in due course to cover, for example, the establishment of contracts over the Internet using digital signatures, liabilities for cross-border electronic transactions, use of customer information and privacy. As facilities and the scope of services improves, banking through the Internet will certainly become more popular. At that stage, it might be appropriate to codify the security objectives and requirements into a more rigorous guideline which all institutions offering Internet banking services should follow.                Meanwhile, Interim examination procedures will cover many of the principles and proposals discussed in this document, so it will be necessary for banks to demonstrate their responses to these issues in the way their Internet banking services are designed and managed.  It is important to remember that many of the major risks are a consequence of poor physical or procedural security, rather than technical weaknesses.  Hence, banks should ensure that both system and process security are properly addressed, and that basic access controls to banking technology buildings and equipment are fully maintained.    SAMA believes that an effective internal auditing function can help a bank detect potentially serious technology-related problems. The auditor should report and be accountable to the Board or its designated committee.  A well-informed Internal Auditor can help to assure a proper control environment for new technology and its operation. This means that controls must ensure that:      Records are being processed accurately and in a safe and sound manner.    Accounting data is reliable.    Operating procedures are efficient and effective.    Procedures are in effect to assure continuity of services.    High-risk conditions, functions, and activities are identified and effectively monitored.    There is proper adherence to management standards and policies, applicable laws and regulations, regulatory statements of policy, and other guidelines.    As Internet banking develops, therefore, SAMA will aim to keep the banks informed of best security practice internationally by issuing enhanced versions of this document to assist in maintaining the safety of on-line banking in the Kingdom.  However, it is the banks’ responsibility to maintain effective internal and technical controls in keeping with these guidelines.      **Appendix 1 – Specific Risk Control Measures**      Ensure the physical security of sensitive computer sites and facilities, by controlling the access of personnel, software and equipment    Deploy secure operating systems    Deploy secure applications and at least SSL to secure payment processes    Change all default passwords for new systems immediately upon installation as they provide the most common means for intruders to break into systems.    Install firewalls between internal and external networks as well as between geographically separate sites.    Create a secure, integrated cryptographic architecture    Develop built-in redundancies for single points of failure which can bring down the entire network.    Engage independent security specialists to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff.    Conduct network/host penetration testing at least annually.    Conduct cryptographic penetration testing    Conduct vulnerability analysis    Use network scanners, intrusion detectors and security alerts.    Implement anti-virus software.    Establish comprehensive security policy and procedures.    Perform comprehensive security monitoring    Maintain comprehensive security logs and audit trails.    Analyse security logs for suspicious traffic and access attempts.    Establish an incident management and response plan.    Test the predetermined action plan relating to security incidents.    Install network analysers, which can assist in determining the nature of an attack and help in containing such an attack.    Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.    Maintain a swift recovery capability at a hot alternative site.    Conduct security awareness education and training programs.    Require frequent audits to be conducted by security professionals or internal auditors who have the requisite skills.    Consider taking insurance cover for various insurable risks, including recovery and restitution costs.    **Appendix 2 - Access security options for bank web servers**  ***Standard client certified web (HTTPS) plus physical token***    Standard web based security offers security functionality with very little impact on the remote workstation and is included within standard web browsers providing a degree of security for Web based communications.    The standard Web security, using SSL, relies on three components to ensure authenticity between the remote workstation and the web server; the Web server, the remote workstation and the end-user. Whereas it is possible to secure the Web server with conventional security controls, it is often difficult to secure the remote workstation, which is often beyond the control of the Web based service. The lack of guaranteed security levels at the various components and a weak authentication method create a number of high risk vulnerabilities which could be exploited to gain unauthorised access to the system or disclosure/modification of sensitive data.    To counter the weak authentication offered by standard Web security it is possible to implement a hardware token device for the user. This token contains security information necessary for a user to authenticate as the user. The token itself can be extremely difficult to clone or attack to extract the private information. Using a hardware token with a PIN protecting the user certificates gives a strong two-factor authentication (something only the user has and something only the user knows).    A service relying on standard Web-based security may be vulnerable to attacks that aim to exploit weaknesses in the configuration of the remote workstation. For example, a remote workstation may implement weak access control allowing data to be extracted from the hard disk over the network with little authentication.    Browser configurations and implementations often obscure the standard security functionality that is operating. This could allow impostor Web servers to masquerade as the host server without the user being aware and could result in data being sent from the user to the impostor site including sensitive documents.      ***VPN Secure client with physical token and application on CD***    Implementation of a hardware token VPN-based solution requires additional software and hardware at the remote workstation. The VPN software is tightly integrated with the remote workstation and server and would require installation of software drivers and might require hardware readers.    A VPN-based solution provides an additional layer of security that gives a increased level of confidence in the authenticity, confidentiality, integrity and non-repudiation between the remote workstation and the host Web server compared to the standard client certified Web solution.    Authentication is based on two factors; something only the user has i.e. the hardware token, and something only the user knows i.e. his PIN or password. This makes capture of user credentials in order to gain unauthorised access to the Web portal extremely difficult.    The VPN software would be tightly integrated with the remote workstation and can enforce VPN communication with the host Web Server. An impostor site would have to steal the VPN certificate from the real Web Server or attack the VPN software in the remote workstation in order for the masquerade to be convincing if a suitable VPN configuration is implemented.    The implementation of the Web client onto a CD adds to the security of the connection by reducing the risk of Trojan horse software and therefore the ability of an intruder to implement a relay or masquerade attack.    Sensitive data will reside on the remote workstation either while the data is being modified or stored. Lost or stolen workstations or workstations that have been compromised may allow sensitive data to be extracted. It is possible that file or disk encryption could be used to protect the data stored on the remote workstation. The VPN client software can be used to protect the remote workstation making extraction of sensitive data over the network much harder.    Use of IPSec[\*](http://212.71.42.15/en/control/procedure/ibsguidelines.htm" \l "_ftn1" \o ") may not be permitted through corporate firewalls and additional firewall configuration may be required. Some proxy-based firewalls may not allow IPSec communication to function through the firewall and an alternative firewall would be required.    ***Risk summary***  The following scattergram shows the location of the risks identified in this section in relation to their vulnerability and likelihood:-      Figure 1. Risk Scattergram   |  |  | | --- | --- | | **Risk Number** | **Description** | | 1 | Weak authentication to host allowing an unauthorised individual to authenticate as a valid user | | 2 | Disclosure of information while in transit between the host and the user | | 3 | Masquerade attack on the portal server and subsequent user login to false host system | | 4 | Relay attack on users of the host system | | 5 | Disclosure of data stored on the remote workstation over the network | | 6 | Disclosure of data stored on the lost/stolen remote workstations | | 7 | Trojan horse attack on the remote workstation | | 8 | Weak audit trails make user accountability difficult |     **Issue matrix**   |  |  |  |  | | --- | --- | --- | --- | |  | **Standard HTTPS with username + password login** | **Standard client certified web (HTTPS) using physical tokens.** | **VPN Secure client with physical token and application on CD-ROM.** | | **1) Weak authentication to host allowing an unauthorised individual to authenticate as a valid user** | Vulnerable | Two factor authentication protecting access to the host system | Strong two-factor authentication protecting access to the initial login screen | | **2) Disclosure of information while in transit between the host and the user** | SSL encrypted | SSL encrypted | IPSec encrypted | | **3) Masquerade attack on the host server and subsequent user login to false portal** | Vulnerable | Vulnerable however captured information cannot be relayed or used by an attacker without a copy of a valid digital ID | VPN configuration can specify the servers that can be contacted. Cryptographic authentication ensures the server is authentic. | | **4) Relay attack on users of the portal server** | Vulnerable | Relay attacks only possible if the private key van be extracted from the hardware token. | Relay attacks only possible if the private key can be extracted from the hardware token or the attack uses a key held within another hardware token to establish the VPN connection between the relay and the genuine portal server |        |  |  |  |  | | --- | --- | --- | --- | | **5) Disclosure of data while stored on remote workstation over the network** | Vulnerable | **Vulnerable** | Vulnerable however disk/file encryption may be bundled together with the secure client software. | | **6) Disclosure of data stored on lost/stolen remote workstations** | Vulnerable | Vulnerable | Vulnerable however disk/file encryption may be bundled together with the secure client software.    Strong authentication to the remote workstation protects data from opportunist data extraction. | | **7) Trojan horse attack on the remote workstation** | Vulnerable | Vulnerable | Vulnerable however the additional software on the client can also be used to harden the configuration of the remote workstation.  The application stored on CD-ROM mitigates the risk associated with the configuration of the applications. |        |  |  |  |  | | --- | --- | --- | --- | | **8) Weak audit trails make user accountability difficult** | Vulnerable | May be possible to tie the username for the portal server together with the client certificate used during establishment of an SSL communication. However, certificates are vulnerable to being extracted and copied. | May be possible to tie the username for portal server together with the client certificate used during the establishment of a VPN session. |       **Appendix 3 – Outsourcing security issues**   |  | | --- | | **Outsourcing disadvantages caused indirectly by lack of proper security policy**  ·        Loss of control  ·        Higher exit barriers  ·        Exposure to vendor risks, including: Financial strength, Loss of commitment to outsourcing, Slow implementation, Promised features not available, Lack of responsiveness, Poor daily quality  ·        Become hostage to “extra use” charge, Difficulties in quantifying economies  ·        Costs of conversion  ·        Attention required by senior management  ·        Supply restrictions  ·        Possibility of being tied to defective technology  ·        Concerns with long-term flexibility and meeting the changing business requirements on a timely basis  ·        Concerns regarding the continuing cost-benefit of outsourcing  ·        Damage to corporate image  ·        Potential liability claims  ·        Lack of clarity over ownership, reporting and control  ·        Concerns regarding industry acceptance  ·        Inadequate technical service quality |       [\*](http://212.71.42.15/en/control/procedure/ibsguidelines.htm" \l "_ftnref1" \o ") IPSec is a standards based protocol for secure communication over Internet Protocol (IP). Unlike SSL IPSec is not usually enabled on corporate firewalls. |