Security Guidelines for Mobile Banking & Payments

DRAFT

15 FEBRUARY 2002 - VERSION 1.1

CONSULTATIVE PAPER

SUBJECT TO CHANGE

CLOSING DATE FOR COMMENTS – 15 MARCH 2002

Enquiry: Tony Chew, Director, Technology Risk Supervision Tel: 2299109

Please email your comments to tonychew@mas.gov.sg

Table of Contents

1. Introduction

1.1 Purpose

1.1.1 The purpose of this document is to enunciate a set of security and technology risk management guidelines for banks and payment service providers who are responsible for the design and delivery of mobile banking and payment services. It aims to provide a framework for security risk assessment and specify control and security standards applicable to the wireless environment for banking and payments.

1.1.2 The business principles and security controls recommended in this document are not intended to be exhaustive nor to prescribe a uniform set of security requirements for all industry participants, banks, merchants, network operators and service providers. These guidelines should be applied in a way that is appropriate to the risks associated with the types and values of mobile products or services being offered, the devices used, the delivery channels chosen and the systems which process the mobile transactions and enable the interactions between customers, merchants, banks and other participants.

1.1.3 There are certain characteristics of wireless technologies which give rise to security implications. Broadly these are:

a. Wireless network connections are, in general, less reliable and slower than their wired counterparts.

b. Processing power and memory capacity in many mobile terminals are constrained.

c. The size of mobile terminals restricts data-entry and display capabilities.

d. Over-the-air transmissions are vulnerable to eavesdropping.

1.1.4 Security is a business issue. Technology solutions, key business principles and strong management commitment play a critical role in establishing a rigorous framework for sound risk management and robust security practices. Information security is fundamental to the reputation of the business and its underlying operations. The ability to develop and maintain

market and customer confidence is contingent upon the adequacy and reliability of security practices.

1.1.5 Wireless technologies, mobile devices, telecommunications networks and computer systems are the basic infrastructure for supporting anywhere, anytime customer service strategies such as mobile shopping, banking and payments. The interconnectivity and interoperability of networks, systems, and applications have expanded so rapidly and dramatically that the need to implement security measures to protect customers and their data has never been more pressing and challenging.

1.1.6 The effectiveness of security risk management is predicated on the ability to identify threats and vulnerabilities and the resultant actions taken to reduce their potency and potential impact to an acceptable level. Customer trust in banking and payment services, including the technologies deployed, is fundamental to the safety and soundness of the financial industry.

1.1.7 This document should be read in conjunction with the MAS Internet Banking Technology Risk Management Guidelines as many of the risk management and security principles espoused therein also apply to the wireless environment.

1.2 Authentication Methods

1.2.1 Authentication is one of the most important security imperatives in verifying the identity of a customer and determining whether he is permitted to access a particular banking account or payment service. In the wireless environment, authentication can be done through one or a combination of the following methods:

a. something the customer knows (PIN, password)

b. something the customer has (card, token)

c. a unique physiological, genetic or physical trait possessed by the customer (fingerprint, voice)

d. a secret or private cryptographic key which the customer can access and use to prove his identity.

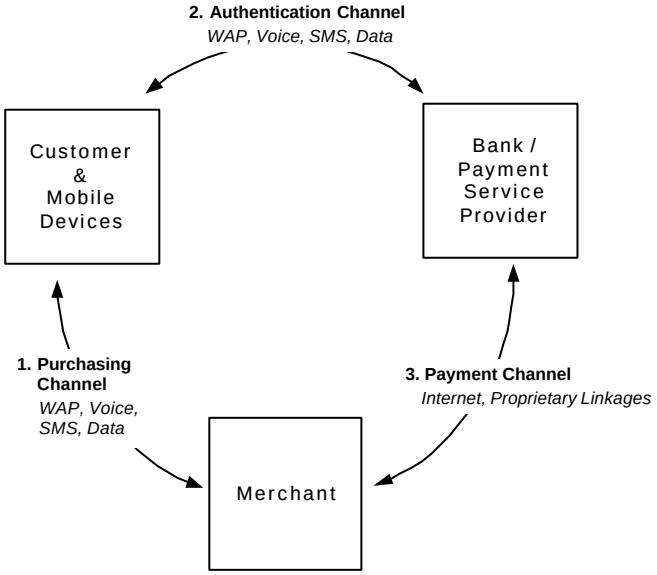

Figure 1 Main participants in a typical payment transaction.

1.2.2 In a mobile setting, the customer's interactions with the merchant, the bank, service provider, network operator and other intermediary entities may involve different service channels such as SMS, WAP, data and/or voice delivery

mechanisms. The purchase interaction with the merchant, access to the bank to effect a payment, the authentication process and execution of the payment transaction may involve multiple steps, distinct delivery channels and separate time segments. Figure 1 above shows the various communication channels by which the main parties interact with each other in a typical payment cycle.

1.2.3 Wireless technologies are characterised by a variety of carriers, service bearers, delivery channels, application functionalities, communication protocols, device capabilities and security attributes. Frequently, they coexist in parallel and are incorporated into systems and networks to provide accessibility and reciprocity between different participants and entities. The authentication process usually requires an exchange of data between the customer, the merchant and the bank (or the payment service provider). This usually entails several steps comprising a challenge and response interaction, and possibly offline confirmatory notifications subsequently.

1.3 PIN Security

1.3.1 Customers should be educated on how to maintain PIN safety and not reveal their PINs to anyone.

1.3.2 Customers should not use the same PIN for different delivery channels or systems as they have different security levels and implications depending on the security risks attached to each of them.

1.3.3 PINs should never be stored or processed in the clear anywhere in a system. Hash values of PINs should be encrypted to guard against brute-force attacks.

1.4 Transaction Logs

1.4.1 Mobile banking and payment systems should maintain detailed transaction logs to enable processing trails to be reconstructed in the event of any disputes or errors. Transaction data including the date and time of the transactions, server IDs, session IDs and customer details should be recorded and retrievable when required. The retention period should be adequate in duration and the storage of this information properly protected.

1.4.2 Security safeguards should be implemented to protect the information from unauthorised modification or destruction.

1.5 Fraud Detection

1.5.1 Banks and payment providers should implement fraud detection systems to identify suspicious transactions or payment behaviour. Appropriate action should be promptly taken to communicate with the merchants and/or customers to resolve any suspicions. Additionally, the detection processes should consider qualitative and quantitative factors such as:

- Profile and demographic details of customers.
- Frequency of usage of payment service.
- Outlets where goods or services are purchased.
- Locality of merchants.
- Payment amounts.

1.5.2 Providers of payment services should develop detailed procedures to facilitate swift investigative actions to resolve reported incidents of fraud or error.

2. Bank Accounts

2.1 Information Services

2.1.1 Banks may offer mobile services that are purely informational: bank advertisements, interest rates, exchange rates and news. Such information is usually available to the public.

2.1.2 Although the risk in such services is low, the information that is provided should be protected against unauthorized modifications. If the information has been deliberately distorted, the bank may encounter customer complaints and reputational damage.

2.2 Bank Account Information

2.2.1 Bank account enquiry functions may be provided through mobile channels. Bank customers may use their mobile terminals to retrieve bank account balances, account summaries, transaction details and other details of a personal and confidential nature.

2.2.2 Banks must take steps to ensure that only authorized parties have access to such information and that the information is conveyed in a manner where confidentiality and integrity is maintained.

2.2.3 In accessing mobile application services, customers may apply for new products, enable or disable features in existing services, personalize their banking interfaces etc. These interactions may involve customers making modifications to their personal profiles such as transaction limits and billing addresses.

2.2.4 In the case of applications for critical banking services or changes to sensitive customer data, banks should initiate follow-up actions to confirm any new information or changes with the customers.

2.3 Transfers Between Customer's Linked Accounts

2.3.1 Customers may link multiple related accounts to their mobile banking facilities which enable them to perform transactions, including fund transfers on all linked accounts. Banks should

allow fund transfers between a customer's linked accounts only when stringent controls are instituted over the linking of accounts to an online mobile service. Accounts should only be linked if they are in the customer's own name or in joint names subject to the bank's prevailing terms and conditions.

2.3.2 System checks and validations should be provided in the online banking systems to disallow and detect unauthorised or erroneous linking of unrelated customer accounts.

2.4 Transfers to Third-Party Accounts

2.4.1 Banks typically provide two types of third-party fund transfer services:

a. Transfers to pre-approved third party accounts.

b. Transfers to third-party accounts without pre-approval.

2.4.2 Transfers to pre-approved third-party accounts should be carried out only if these accounts have either been registered by the bank itself or if customers have given their banks specific written instructions and authorisations to do so. Examples of bank pre-approved accounts include, but not limited to, government agencies and other reputable billing organizations.

2.4.3 Transfers that do not require pre-approval enable bank customers to send their money to unrelated accounts within the same bank or at another bank. Such transfers pose a high level of risk as they result in the immediate movement of funds from one customer account to another. Transaction limits should be imposed as risk-reduction measures. Where such transfers are liberal and flexible, additional security measures such as two-factor authentication should be considered.

2.5 Mobile Payment Services

2.5.1 Banks can provide mobile payment services to enable their customers to make direct payments from their bank accounts (cheque, savings or debit/credit card accounts) to merchants or third parties.

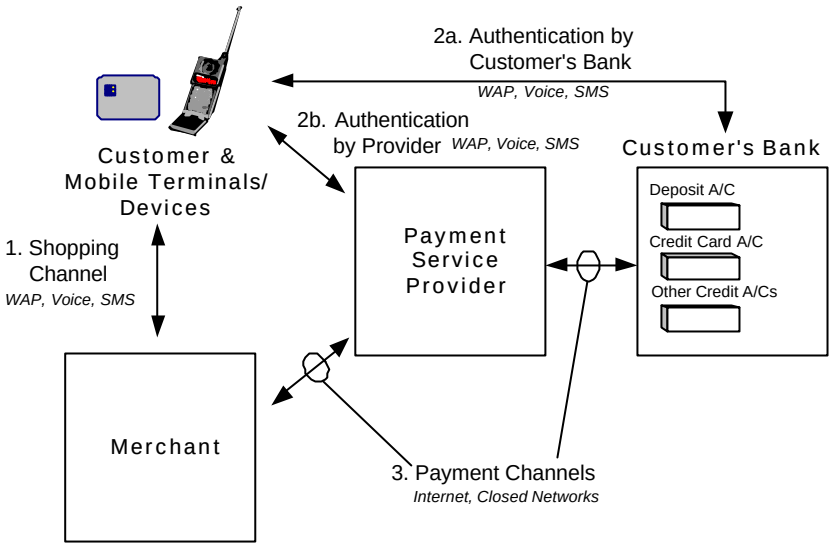

Figure 2 Illustrative Payment Model using Bank Accounts.

2.5.2 Figure 2 shows a mobile payment model based on payments being made from a customer's bank account . There are two scenarios in which the customer's bank account can be debited for payments. The first is where the customer is authenticated by the bank in order to enable the customer to access his account online to effect a payment.

2.5.3 In the second scenario, the customer authorises a third party to raise a debit against his account. The customer also informs the bank about the arrangement and seeks its approval to accept such debits against his account by a third party. This may occur when the customer makes use of bill payment functions provided by a third party. Another way this can occur is when a merchant or a payment service provider switches the customer to his bank so that he may directly effect a payment transfer from his account to that of the other party.

2.5.4 In all cases, the bank must authenticate its own customer before allowing him access to his own account. The bank should not allow nor rely on third party authentication of the bank's own customer.

2.6 Payments Through Third Parties

2.6.1 As a general rule, banks should directly authenticate their own customers in respect of wireless payment transactions made.

2.6.2 Customers may, however, give their banks specific standing authorisations to accept payment debits from specified providers or third parties to charge the customers' accounts. Such arrangements could, for example, be made through Direct Debit Authorisation (DDA) agreements.

2.6.3 When operating under these arrangements, third parties or service providers should neither obtain nor store the customers' personal banking IDs or PINs for the purpose of raising debit transactions against the customers' bank accounts. Banks should implement strong verification and fraud detection measures to check third party debits against their customers' accounts.

2.6.4 The use of credit and debit cards for making mobile payments normally involves the issuing bank in performing online checks to verify the validity of the card number and expiry date, and utilisations against balance limits. In broad terms, the issuing bank is not required to directly authenticate the cardholder under the terms and conditions governing the use of credit and debit cards.

3. Stored Value Accounts

3.1.1 Stored value accounts (SVAs) maintained by payment service providers go by different names such as e-wallet accounts, virtual card accounts and easy-pay accounts. Customers transfer funds into these accounts for the purpose of making periodic or frequent payments.

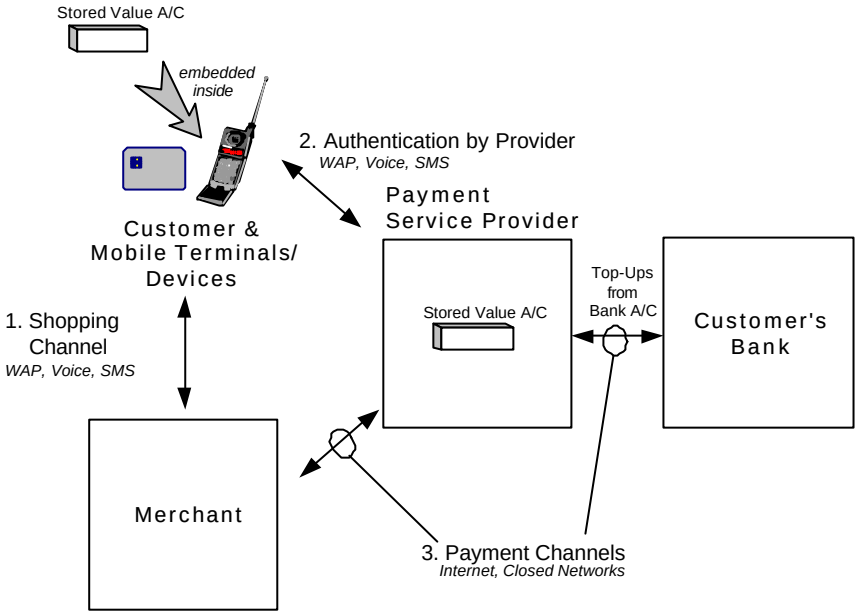

Figure 3. Illustrative Payment Model using Stored Value Accounts.

3.1.2 As shown in the illustrative payment model in Figure 3, SVAs may reside on a service provider's system or on mobile devices. No bank account is accessed in making a payment. Bank accounts, in this model, are only used for replenishing SVAs at the customer's direction.

3.1.3 Payment service providers need not be banks, but they are participants in the financial industry. As such, their ability to conduct business in a safe and reliable manner will affect public confidence in the financial sector as a whole. Conversely, security breaches, systems failures and transaction errors attributable to them will likely tarnish the industry's reputation. Security, therefore, should be a matter of serious concern to these payment providers.

3.2 Customer Authentication

3.2.1 Payment providers should employ adequate security measures to ensure that their customers' sensitive data, especially authentication credentials, are protected. They should provide end-to-end PIN encryption wherever possible. Additionally, strong encryption should be employed to ensure the confidentiality and integrity of transactions.

3.2.2 Some payment products feature automatic top-up of SVAs from customer nominated bank accounts whenever their SVA-balances fall below pre-set balances. Top-ups are considered automatic if, following initial registration for the service, no further authorisation or action from the customer is required for their execution.

3.2.3 Such arrangements effectively make SVAs temporary buffers or proxies for the respective bank accounts of customers. A stream of fraudulent top-ups could, in the absence of other controls, deplete customers' linked bank accounts.

3.2.4 Payment providers offering these automatic top-ups for SVAs should incorporate risk-reduction features into their products so as to limit the frequency of top-ups and, where appropriate, the maximum quantum of each top-up. These measures will reduce the risk of unauthorised top-ups from affliated bank accounts and give account holders more time to detect and to react to unauthorized transactions.

3.2.5 The frequency and risk of unauthorised top-ups may be controlled by implementing transaction-limits, cumulative daily limits and, if appropriate to the provider's business, restricting the uses of SVAs.

3.3 SVA Limits & Restrictions

3.3.1 A general risk-reduction measure is to limit the amount of money that may be at risk. There are three types of limits which may be applied: transaction limits, cumulative limits and account-balance limits.

3.3.2 Transaction and cumulative daily limits are good risk control measures for payment services because they limit the exposure of SVAs in event of fraudulent usage. Overall account balance limits should be placed upon SVAs at levels

that are commensurate with the strength of the payment provider's risk management controls and security practices.

3.3.3 In payment services, such limits may be also combined with restrictions on the purposes to which funds in SVA's may be put to. This should lower the risk of fraudulent payment even more.

3.4 Close Proximity Wireless Payments

3.4.1 Close proximity wireless payment services are typically intended for over-the-counter retail payments. Such transactions should be completed only after customers have given explicit authorisations at points-of-sale. In the absence of such authorisations, it is possible that customers' funds may be involuntarily deducted from their SVAs. For example a merchant could, in a poorly designed system, use short-range wireless technology to cause a passer-by's money to be fraudulently deducted without that person's knowledge.

3.4.2 Explicit authorisation may be any volitional action on the part of the customer in response to a payment request. Examples of such actions include orientating a mobile device towards a reader, pressing certain buttons on the device, pressing keys on the merchant devices and entering customer ID, including customer PIN if necessary.

3.5 SVAs without Limits

3.5.1 Although the risk that such transactions pose to SVAs is high, there may be valid business reasons for providing them. Such services should be protected by the use of authentication processes going beyond a single password.

3.6 Customer Registration

3.6.1 In operational models where payments are not anonymous, potential users must first apply to be registered with a provider before they can perform transactions. During registration, the user will typically submit his/her personal details including name, address, mobile phone number, preferred settlement accounts, etc.

3.6.2 Before approving the application, the provider must exercise due diligence in performing independent background checks

and verifications so as to ensure the authenticity and accuracy of the submitted information.

3.6.3 Customers should be informed in clear and precise terms of the rights, obligations and responsibilities of all parties entering into the payment relationship and arrangements. These issues must be addressed as to normal transactions as well as to processing errors or security problems.

3.7 Tamper-Resistant Stored-Value Devices

3.7.1 Where SVA data resides primarily or substantially in mobile devices/terminals, providers should ensure that the devices are tamper-resistant and would not yield or display any cryptographic keys or other sensitive data. Additionally, the systems and processes that debit or credit these SVA balances must be protected. These measures are necessary to ensure that SVA balances are not susceptible to unauthorised access and fraudulent deductions.

4. Technology Risk Management

4.1 Security Issues

4.1.1 Security threats in the wireless environment are similar to those existing in computer networks and the internet environment. These include intrusion raids, denial of service attacks, viruses, worms, Trojan horses, identity theft and other forms of malicious or fraudulent acts. There are also other manifest security challenges in delivering banking and payment services through wireless channels. Banks and other providers must implement security measures that adequately address these risks and threats regardless of the underlying network and carrier infrastructure used in delivering their services.

4.1.2 The security protection provided by underlying network and carrier infrastructures at the transport level cannot be considered adequate for confidential and sensitive data, particularly PINs and passwords. Examples of such infrastructure include GSM, GPRS, 3G, Bluetooth, Wi-Fi 802.11b and IrDA. At the wireless network level, GSM A5 encryption is weak and has been cryptanalysed. Reliance should not be placed on such proprietary cipher. Although different wireless technologies pose different application, delivery and bandwidth constraints, the major security issues are similar for all of them.

4.1.3 Given the dynamic nature and magnitude of security threats in the wireless environment, it is vital that mobile banking and payment service providers perform periodic independent security vulnerability assessments of their systems. These reviews should be carried out before launching new services and thereafter at least once a year, or whenever there are significant network, application or system changes, or after major security incidents have occurred. To facilitate such reviews, security architecture information should be documented and updated regularly.

4.2 Data Confidentiality

4.2.1 There are, typically, some security mechanisms designed and incorporated into mobile telecommunications infrastructures to protect the confidentiality and integrity of data transmitted over

the air. These basic transport layer security mechanisms cannot be considered sufficient for banking and payment services. End-to-end application layer encryption of sensitive customer details and authentication data, such as PINs, should be implemented.

4.2.2 End-to-end application security means keeping intact the encryption of sensitive data such as PINs, from the data-entry device right through to the host end. PINs must not be transmitted or processed in the clear anywhere in the network systems, servers, gateways or other delivery channels. Encryption, decryption and related authentication processing functions should be carried out in HSM or similar tamper-resistant devices are built specifically for crypto operations.

4.3 System and Data Integrity

4.3.1 Software for wireless applications should implement adequate measures to prevent duplicate transactions resulting from intra-session delays or session failures. Such problems may occur when customers move from areas with good wireless coverage to those where coverage is fragmentary.

4.3.2 Wireless infrastructure including operating systems, carrier channels, various types of applications, mobile terminals, gateways, servers, hosts and processing facilities are vulnerable to hacking, malicious mobile codes, such as viruses and worms, and other kinds of malicious attacks. Providers should therefore install adequate security measures, firewalls, intrusion detection systems, surveillance control procedures, and fast recovery capability.

4.3.3 Providers should implement integrity checks on systems, files and code to ensure the reliability of their systems and that all changes to them have been properly authorised.

4.4 Authentication and Non-Repudiation

4.4.1 When customers are required to provide their passwords or PINs, these should be one-way function hashed or encrypted immediately at the point of input. No sensitive data is allowed to be displayed as clear text on the mobile terminal. For additional security, authentication methods based on more than one factor should be utilized where warranted.

4.4.2 Providers must ensure that encrypted and authenticated sessions remain intact throughout the duration of their communications with their customers. Authentication processes should be repeated after session failures and subsequent resumptions caused by line drop-outs or interrupted connections.

4.4.3 Providers should also consider implementing features in their services that will enable their customers to authenticate them. This is to give customers the added confidence that they are actually dealing with their intended provider. One way this could be done is for the provider to display or replay personal messages that have been input earlier by the customer. These messages are shared secrets between customers and their providers. In order to retain the strength of such arrangements, customers should be advised to change their personal messages at regular intervals.

4.4.4 Details of all transactions, including those that are incomplete or aborted, should be logged. These logs should be reviewed daily for abnormality or aberrations that might constitute security events.

4.5 System Availability and Recoverability

4.5.1 Mobile solutions that provide session management should implement session persistence or session reconnect features. Additionally, sessions should only be valid for periods of time that are appropriate to the security attributes associated with the channel connection.

4.5.2 Providers of mobile services should ensure that they have proper recovery and back-up plans so that disruption to services due to system failures may be kept to a minimum. Such plans should also cater for single points of failure and incorporate requirements relating to standby hardware and alternate facilities to ensure recoverability and high system availability.

4.5.3 Close monitoring of mobile traffic vis-à-vis system capacity is required to ensure that any service degradation due to capacity problems can be addressed in a timely fashion.

4.6 Key Management

4.6.1 Proper key management is important to the effective use of cryptography and digital certificates. Providers must put in place adequate control measures and procedures to enable crypto keys to be created, stored, distributed, replaced, revoked or destroyed securely.

4.6.2 Periodic audits and compliance reviews should be carried out to maintain a high degree of confidence in these security processes. These are especially important when keys are loaded into customers' mobile devices by third parties or device manufacturers on behalf of financial service providers.

4.7 Wireless Application Protocol (WAP)

4.7.1 The use of WAP 1.x gateways creates security concerns due to the "WAP Gap" issue. The "gap" is the result of the transition from WTLS to SSL/TLS that takes place on such servers. PINs and other confidential information are processed in the clear during this conversion period. This vulnerability can be effectively overcome by deploying end-to-end application layer encryption. Mere reliance on physical security to protect WAP gateways is inadequate.

4.7.2 Where WAP gateways are installed, providers should adopt good control mechanisms in and around them:

a. WAP gateways should not process or store highly confidential data such as customer PINs in cleartext form.

b. Cleartext content in the gateway should be erased from internal memory as quickly as possible to reduce the duration of security exposure.

c. Adequate physical security should be implemented to ensure that only authorized administrators have access to gateways and their system consoles.

d. File and system integrity checks should be implemented to detect unauthorised changes or intrusions.

e. The gateways should be placed in firewall-protected network segments, augmented with intrusion sensors, surveillance procedures and other network security mechanisms.

f. Appropriate hardening procedures should be adopted to keep gateway server operating systems at up-to-date patch levels.

4.7.3 End-to-end encryption for addressing “WAP gaps” can be achieved by using WMLScript-based cryptographic functions or by the combined use of WMLScript commands and SIM-Toolkit functions. In the case of WAP 2.0 implementation, a TLS/SSL tunnel can be established so that entire session is encrypted from the customer mobile device to the host system server. This technique still leaves the data exposed in the web server. Therefore, end-to-end application-based encryption is still necessary. WAP2.1 defines an application level encryption using the WMLScript EncryptText function to achieve encryption security beyond the web server to the host system endpoints.

4.7.4 Continuing advances in wireless technologies have provided increasing opportunities for telcos, network operators, service providers and banks to use public key cryptography for establishing security platforms and authentication solutions. Though PKI/CA standards have been evolving and improving in recent years, the high cost of implementation has inhibited widespread development and deployment. Demand for WPKI poses even more questions and challenges. Low bandwidth, high latency and limited processing capability in mobile systems and devices pose formidable barriers to the implementation of digital certificates and asymmetric signatures.

4.7.5 Both WAP and SMS are capable of providing the authentication channels to support asymmetric signature operations. WPKI vendors and network operators offer various services, products, programming development toolkits and interfaces to support the following:

a. installation of CA root keys in WAP servers and mobile devices.

b. generation of public/private key pair and implanting the private key in WIM or SWIM chip cards.

c. registration and issue of device, client and WTLS certificates.

d. WMLscript SignText function for generating digital signatures.

SMS STK browser is also capable of producing digital signatures.

4.8 Short Message Service (SMS)

4.8.1 SMS is a store and forward service that is inherently insecure because the messages are transmitted in the clear and stored in the clear at an SMS Centre before being forwarded to their intended recipients. SMS often suffers from latency problems. Time critical transactions should not rely on SMS channel.

4.8.2 SIM Toolkit (STK) technology can be used to provide encryption security to the SMS channel such that data in transit is protected all the way from the mobile device to the SMS Centre. However, this is a transport layer security mechanism. It does not provide end-to-end confidentiality for customer PIN and other sensitive data from the mobile device to the final host system endpoint.

4.8.3 Additional procedures for improving SMS security might include customers checking their personal assurance messages and the provider in turn verifying the registered phone numbers of customers.

4.9 Interactive Voice Response (IVR)

4.9.1 Mobile IVR services are potentially vulnerable to eavesdropping through OTA interception of calls. Thus IVR system should not be used for high-risk or high-value services. All IVR sessions must be recorded including the caller's phone number, the sequence of transactions made by a customer and any voice transaction details. PIN or authentication data should not be logged.

4.9.2 In accordance with the security practice of using different PINs for different systems with varying security levels, customer should use a separate PIN for IVR access. If voice recognition technology is deployed, voiceprints of customers should not be the only factor of authentication as the current state of technology is still immature. Another factor should be required to properly authenticate customers.

4.9.3 PINs entered during an IVR transaction must not be broadcast over a voice-to-digital coupler such that it can be heard by customer service personnel participating in operator-assisted transactions. Customer PINs should, upon leaving the IVR system, be encrypted so that they are not vulnerable to sniffing, interception or modification before reaching the host backend system for verification.

4.9.4 On some mobile phones, PINs entered may be recalled through redial menus. Instructions should be given to customers to erase PINs from the phone memory to prevent PIN discovery by accessing previously dialled numbers.

4.9.5 Banks and payment service providers should educate their customers on the use of PAM[1] to enable them to safely check the authenticity of the connection

4.9.6 Mobile service providers should provide clear configuration instructions if their customers are required to manually configure their own mobile terminals.

[1] A personal assurance message (PAM) is given to the service provider during registration so that the customer can authenticate the provider. Customers should be advised or prompted to modify their PAM's periodically to ensure that they retain their value as shared secrets.

5. Security Practices

Banks and payment service providers should comply with the following security principles and practices:

5.1 PIN Security

5.1.1 Implement minimum 6-digit customer PINs.

5.1.2 Protect customer PINs using end-to-end application layer encryption.

5.1.3 Do not allow PINs to be in the clear anywhere in the network or system.

5.1.4 Authenticate customer PINs in tamper-resistant hardware such as crypto-servers or hardware security modules (HSM).

5.1.5 Encrypt the hash values of customer PINs randomised with a salt.

5.1.6 Do not store customer PINs anywhere.

5.1.7 Differentiate PINs for different channels of different risk levels; advise customers to use different PINs for different channels.

5.2 Network and System Security

5.2.1 Use strong encryption for protecting confidential information in transit.

5.2.2 Implement application layer encryption over network transport layer encryption for critical information.

5.2.3 Establish firewalls, intrusion sensors, data file and system integrity checking, surveillance and incident response procedures.

5.2.4 Conduct risk management analysis, security vulnerability assessment and penetration testing at least once annually.

5.2.5 Conduct risk and security assessment of new products, services and systems before they are launched.

5.2.6 Maintain adequate documentation of security practices, methods and procedures used in mobile banking and payment systems.

5.2.7 Implement appropriate physical security measures to protect system gateways, network equipment, servers, host computers and other hardware from unauthorised access.

5.3 Cryptographic Key Management

5.3.1 Protect all cipher keys against unauthorised access; do not allow anyone to know an entire key (master keys must be separated into different components such that no individual has full knowledge of and access to all the components at the same time).

5.3.2 Use tamper-resistant devices for storing encryption keys

5.3.3 Implement strong physical access controls on equipment used to generate, store and archive keys.

5.3.4 Employ segregation of duties for the custody of keys and key management processes.

5.3.5 Perform key generation in secure tamper-resistant devices.

5.3.6 Enforce activation and expiration periods for keys.

5.3.7 Inform customers of cryptographic key revocation process in the event that the keys are lost or suspected of having been compromised.

5.4 General Security Practices

5.4.1 Implement security measures to segregate internal from external networks and telecommunication infrastructure.

5.4.2 Issue and maintain comprehensive information security policies relevant to the mobile banking and/or payment services.

5.4.3 Implement intrusion detection system to detect and record intrusions, security breaches or weaknesses.

5.4.4 Deploy effective fraud monitoring systems and processes.

5.4.5 Implement transaction, cumulative and/or account-balance limits to mitigate risk exposures.

5.4.6 Establish confirmatory procedures for high value transactions.

5.4.7 Maintain detailed transaction and system logs.

5.4.8 Employ Personal Assurance Message (PAM) for SMS and IVR services.

5.5 Customer Education

5.5.1 Advise customers to use different PINs for different online services.

5.5.2 Provide instructions to customers on how to configure their mobile devices to access mobile banking and payment applications.

5.5.3 Advise customers to take security precautions in using mobile banking and payment services.

5.5.4 Advise customers of dispute handling, reporting procedures and the expected time for resolution.

5.5.5 Avoid the use of abstruse legalese and technical jargon in communications with customers.