Oman National ATM/POS Switch Network

OmanNet Operating Rules

Technical Book 2 - Security Frame Work

Table of Contents

Change Control

Document Amendment Record			
Change No.	**Date**	**Prepared by**	**Brief Explanation**
Version 1	December 2010	CBO PSD	Initial Version
Version 1.1	January 2014	CBO PSD	Revised for EMV Section 1.2 PIN Management revised to include Offline PIN Section 1.3 Key Management revised for Public/Private key on the terminal
Version 1.2	February 2014	CBO PSD	Section 2.3 Key Exchange Key (KEK) Components revised for Key Exchange Section 2.6 KEK Generation/Update Procedures revised for member bank generation and update of keys Section 2.7 Duties of the SST at the OmanNet Switch revised for SST team responsibilities from OmanNet perspective Section 2.8 Duties of the Member Bank Custodians at the Switch added as part of member bank custodians duties Section 2.9 Duties of the Member Bank Custodians at the member bank split and revised for member bank custodian duties
Version 2.0	February 2014	CBO PSD	Section 1.3 Key Management revised for Key Exchange frequency Second Release

© 2014 Central Bank of Oman

All rights reserved. All information contained in this document is confidential and proprietary to the Central Bank of Oman. No part of this document may be photocopied, electronically transferred, modified, or reproduced in any manner without the prior written consent of the Central Bank of Oman.

All brands or product names are trademarks or registered trademarks of their respective companies or organizations.

1 Network Security Standards:

1.1 Introduction:

This section includes the OmanNet Network Security Standards. The primary audience of the security framework document is the staff of both OmanNet and the associated member banks. It is assumed that the readership has a basic understanding of security.

Each member bank will be represented on the OmanNet security committee, which in turn will have regular meetings to discuss issues as they come up. This section contains the security standards for:

- Key management
- PIN management
- Access control

Each Member having a proprietary network shall implement the security requirements for the protection of the network transactions in their own network.

Members exchanging or processing transactions shall be responsible for the security of the transactions (including the PIN), to guarantee that events are within their reasonable control.

Acquirers must implement means to verify the authenticity of the devices connected to the network. It is the Acquirer's responsibility to ensure that all of the network's service transactions they introduce to the network are originated from an authorized terminal.

All participants in the network should maintain cardholders' personal information as confidential. Only financial and other supporting information, which are required for completing, tracing, reversing or correcting a transaction may be passed to participants.

1.2 PIN Management:

PIN issuance: The Issuer shall have a secure system for issuing and conveying PINs to cardholders and to allow cardholders to select or change their own PINs.

The Issuer system shall ensure the following:

- PIN is always encrypted to all but the cardholder
- PIN is securely delivered to the cardholder
- The cardholder is allowed to change his/her own PIN in a secure and controlled environment

The Issuer shall convey to their cardholders the importance of exercising constant care and diligence in protecting the confidentiality of their PINs.

The PIN must be composed of a set of numeric digits, the minimum length of a PIN should be 4 digits, while the maximum PIN length is up to 12 digits.

For ICC (chip) cards, there are two types of PINs:

- Online PIN: it is used to verify the cardholder online during the transaction by the issuer authorization host

- Offline PIN: it is used to verify the cardholder offline during the transaction by the ICC

Issuers supporting offline PIN on the ICC must ensure that the offline PIN is synchronized with the online PIN during PIN issuance, i.e. the PIN value must be the same for offline PIN and online PIN.

In addition, issuers should provide proper mechanisms to keep the Online PIN and Offline PINs in sync in case PIN change is to take place.

PIN entry requirements: A PIN entry device should be provided to allow secure entry of the PIN by the cardholder. This device should conform to any applicable standards on the particular environment.

The Acquirer is required to ensure the following:

- Adequate protection against disclosure of a cardholder's PIN during PIN entry. The PIN entry environment shall be designed to minimize the risk of PIN disclosure
- Protected location of the Secured PIN Entry Device (SPED) Keypad to minimize the potential for disclosing the PIN during entry
- Cardholder PIN entry should be performed in accordance with payment system brand requirements that relate to the PCI PTS Program

PIN Keying Rules:

For Keying in a PIN, the following rules should be followed:

- The first PIN character entered should be considered the left-most character and the final character the right-most character (ref. ANSI X9.8)
- An 'Enter' Key or equivalent Key should be used to signal the end of PIN entry
- The entered PIN should not be displayed on the screen; relatively, a string of insignificant symbols such as asterisks should be displayed to indicate the number of characters received. Where PIN entry is accompanied by an audible sound, the sound for each character must be of the same frequency and tone (identical sound for all keys)

PIN encryption requirements:

Except during customer entry, PINs must always be encrypted when unconfined to a Physically Secure Device (PSD).

Online PIN encryption must only occur with one of the allowed key-management methods:

- DUKPT
- Fixed key
- Master key/session key

Online PIN must be encrypted using an algorithm and key size that is specified in ISO 9564. The current approved algorithm for online PIN is 3DES using the Electronic Code Book (ECB) mode of operation as described in ANSI X9.65.

The online PIN encryption process must be conducted as follows:

- PIN encryption, decryption, translation and format changes must occur within a PSD, except during PIN entry, where PIN encryption may be performed in a Secure PIN Entry Device (SPED)
- The encryption process must be reversible (ref. ANSI X9.8), 1995, ”Balancing – Personal Identification & Management &Security“
- The PIN must be in the form of an ANSI PIN block format (ref. ANSI X9.8) 1995, ”Balancing – Personal Identification & Management &Security “
- PINs must be encrypted under PIN Encryption Keys known only to members of the Transaction
- PINs should be encrypted immediately after their complete entry triggered by pressing the “Enter” or its equivalent equivalent Key

Note: Unencrypted PINs should not be kept in any form of database. Only a reference number called the PIN offset is kept in a customer database for PIN verification

Offline PIN Encipherment should be supported using ICC unique public key pair consisting of a public Encipherment key and the corresponding private decipherment key.

Terminal perform Offline PIN encipherment using an asymmetric based encryption mechanism in order to ensure the secure transfer of a PIN from a secure “tamper evident” PIN pad to the ICC.

PIN verification requirements:

Online PIN verification includes the following requirements:

- The cardholder should use a valid card and PIN in order to initiate a transaction
- The PIN entered by the cardholder must be verified at the time of the transaction. The Issuer side (ICC or Authorization Host) should be the only party responsible for PIN verification (refrains X9.8).
- It is the responsibility of each issuer member bank to determine the manner in which the cardholders’ PINs are to be verified
- The cardholder must enter the PIN and must be permitted a predefined number of consecutive attempts to enter the correct PIN for one Transaction. The issuer must take action after any additional consecutive PIN failures to decline the transaction, block the card from being used, or capture it.

Offline PIN verification includes the following requirement:

- Decipherment of Offline PIN is performed by the ICC using the private component of the asymmetric key for verification.

Additional Requirements:

The acquirer member bank should ensure that:

- Data encoded on the card’s magnetic strip and the data personalized on the ICC will not be disclosed to anyone other than a member bank that is a party to the transaction
- Such data may not be used for purposes other than completing a transaction

- An ATM vault should be secured. No one can access it except ATM officers assigned by the acquirer member bank. An ATM vault should be accessible only for replenishing and maintenance.
- The complete PAN shall not be printed on the receipts

1.3 Key Management:

The key management is covering several factors such as key generation, key distribution and key storage. The following cryptographic keys are required:

- LMK (Local Master Key) also referred to as MFK (Master File Key) which is the encryption key stored within the Host Secure Module (HSM). LMK is used for the following :
  - Encrypt other cryptographic keys for local storage
  - Securely translate keys from local encryption to zone key encryption for export and import
  - Encrypt & Decrypt PIN data
- ZMK (Zone Master Key) which is the Key Encryption Key (KEK) used between OmanNet and member banks switches. ZMK or KEK is used to encrypt Zone Working Keys when those keys are transferred between two parties sharing an encryption infrastructure
- ZWKs (Zone Working Keys) used for PIN and MAC processing

1.3.1 Key Generation:

Key generation process must always be conducted in a secure environment to prevent any kind of risk. Logically the key generation is always occurring within a physically secured device such as HSMs:

- The generation of the keys (LMK, ZMK, ZWKs, and public/private key pairs) should be random or pseudo-random
- A unique key should be used for one specific cryptographic purpose only; in addition, a key should not be intentionally equal in value to any other Key

After generation, the LMK must be managed securely by minimum of three trusted banking officers.

All other keys must be generated and encrypted randomly in a single operation using the HSM. After which, the encrypted keys should be stored in a secure database.

1.3.2 Key Exchange:

- ZMK will be exchanged manually between OmanNet and the corresponding member bank
- ZMK is always kept encrypted under the LMK within the switch database

- A set of smart cards including the ZMK components and its key check value (KCV) will be sent out to the member bank (details of the ZMK exchange procedure are fully described in the following section "Key Encryption Key Procedures")
- Under ZMK, two ZWKs will be exchanged; the ZPK and ZAK. The ZMK is used to exchange the ZPKs and to exchange the ZAKs
- The key exchange will be done through network management messages (1804) to exchange the working keys where Data Element 96 will specify the key that is being exchanged (for details regarding the content of the Data Element 96, check the MBI specification)

When member bank receives the key exchange message, they should utilize the HSM to translate the new key (ZWK) from encryption under ZMK to encryption under the bank's LMK.

The output from the HSM is the ZWK encrypted under the LMK along with its checksum. The first four characters of the check digits produced by the HSM are compared with the check digits in the 1804 message (key exchange message).

- If they are the same then the translation is successful. Consequently, the member bank must take the newly translated key and store it in an encrypted version in a secure database

Finally, the member bank must reply with 1814 response message indicating the result by assigning the appropriate response code in the message.

Key Change Frequency Requirements:

A mechanism must be in place and implemented to change all Keys that may be affected when it is known or suspected that security has been compromised.

Specifically, a Key must be changed when:

- A Key Synchronization Error has been detected
- It is known or suspected that the Key has been compromised
- The number of MAC failures exceeds the number considered acceptable by the member bank

Timers will be set for the dynamic Key exchange between the Switch and the member bank. Minimum Key change frequency requirements are as follows:

Type of Key	Between member bank and Switch	Bank proprietary network
ZPK, and ZAK	1440 sec[1]	Bank's Discretion
Zone Master Key	Bank's Discretion	Bank's Discretion

Table 1- Minimum Key change frequency requirements

[1] The period of time after which OmanNet forces a Key Exchange, this period of time is subject to change based on OmanNet discretion

1.3.3 Keys Synchronization:

The synchronization of the keys (ZMK, and Zone Working Keys [ZPK and ZAK]) is required periodically to avoid issues and minimize the denial of the service caused by working keys being out-of sync (ZPK and ZAK).

The solution to avoid any synchronization issue for Zone Working Keys is to maintain two copies of the working keys, current key and old key. The old key is kept for configurable period of time to allow for transactions processed with the old key to be handled:

- For every member bank there will be two working keys (A, and B)
- Only one of them should be active at a time
- If key A is used, and there is a key exchange, key A should not be overwritten, but key B will be the new active key
- For every transaction sent, the key index (A or B) will be included in the message
- If key A is the current active key and a request for key exchange is received, key B will be the new working key
- Old key A is kept for a configurable period of time, known as the grace period within which transactions with old key A can be processed
- After the grace period, key A will be removed, and no transaction with the old key A will be processed
- Exchanging the key will work in a round robin algorithm, A-B-A

Exceptions

One exception should be handled to avoid any out-of sync errors, when the switch is sending a transaction to the issuer (transaction flow is initiated by OmanNet switch) and prior to receiving a successful response on the key exchange request from the issuer side, the switch should send the transaction with the old key and not the new one.

1.3.4 Key Storage Requirements:

Key storage requirements are as follows:

- ZMK components must be stored on smart Cards with three officers (referred to as Key Custodians)
- Control with split knowledge
- ZMK must be stored as cipher text Keys confined to a Physically Secure Device

All other types of Keys must be stored as cipher text, encrypted under the bank's LMK.

1.3.5 Key Destruction:

Plaintext Keys or Key Parts no longer required must be destroyed. The Key destruction procedures are as follows:

- Printed Keys and Key Parts must be destroyed by cross-cut shredding, burning or pulping
- Plaintext Keys and Key Parts stored on other media must be destroyed to make it impossible to recreate them by physical or electronic means

1.3.6 Keys Definitions:

1.3.6.1 Local Master Key - LMK:

LMK is the master key per secured device; all other keys are encrypted under this key within the switch database, it is also referred to as Master File Key (MFK).

LMK components are written to smart cards protected by a PIN. It's the responsibility of each member bank to ensure safe guarding of these cards and its backups are kept in a secured different place. A minimum of 3 trusted bank officers (Key Custodians) should be involved in the LMK generation and maintenance process. No single officer should have the access to any component other than their own part.

Since the bank's LMK is used to generate the bank's other keys, it serves as the ultimate key in the bank's key encryption system. If LMK was compromised by an unauthorized person, then the member bank must replace all of its encryption keys.

1.3.6.2 Terminal Master Key - TMK:

The TMK is a key-encryption key used to encrypt other TMKs or keys of lower level for transmission. It is stored encrypted under one of the LMK pairs.

TMK falls under the responsibility of the member bank, where TMK is shared in a similar way to ZMKs but between ATM/POS Acquirers and the ATM/POS. The TMK requires being securely loaded as components into the ATM/POS.

1.3.6.3 Terminal PIN Key - TPK:

The TPK is a data-encryption key used to encrypt PINs for the purpose of transmission; it is used within the local network of the member bank. For transmission, the TPK is encrypted under a TMK. It is stored encrypted under one of the LMK pairs.

At ATMs, TPKs are used to encrypt a PIN/PAN block after a PIN is entered by a cardholder.

1.3.6.4 Terminal Public Keys:

This is the responsibility of the member bank, where the Public Keys are received from the respective International Payment Network (Visa or MasterCard) to be updated at the terminal.

1.3.6.5 Zone Authentication Key - ZAK:

The ZAK is used to create MACs on messages between parties.

1.3.6.6 Zone Master Key (ZMK) or Key Encryption Key (KEK):

The ZMK/KEK is used to securely transport and store other cryptographic keys. This key is used to package and ensure that keys are not compromised during the transport process between parties.

The ZMK/KEK is a shared key that is exchanged between two parties by the Key Custodians. Once this key is successfully exchanged, it will be used for exchanging new keys securely in an automated fashion.

A ZMK/ KEK will be established with each of the member banks. During the setup process, ZMK/KEK components will be produced in a similar way to the LMK. ZMK/KEK components are delivered to trusted bank officers/custodians within the member banks via a set of smart cards.

Once the ZMK is set up, it will be used for encrypting Zone Working Keys (ZWK), which are the ZPKs and ZAKs. In this way, new working keys can be securely generated and transmitted to sharing parties at regular intervals. The ZMK itself will be replaced at pre-defined intervals.

1.3.6.7 Zone PIN Key - ZPK:

The ZPK is a data-encryption key used to encrypt PINs before being transferred between two parties. For transmission, the ZPK is encrypted under a ZMK. It is stored encrypted under one of the LMK pairs

1.3.6.8 Zone Working Key:

Zone Working Keys are referred to ZPKs or ZAKs. They are keys used for PIN encryption ZPK and for MAC'ing ZAK. ZWKs are generated using HSM and exchanged under ZMK encryption.

1.4 Access Control:

Logical and physical controls must be implemented for key Databases and electronic logs containing magnetic strip and ICC read data. Additionally, except for Terminal Security Modules, physical access controls should also be implemented for host Security Modules restricting access to authorized personnel only.

OmanNet system will classify users according to their functions and the access privileges granted to each user class. The system will contain the following types of users with their functions:

- Scheme Owner: For Creating database objects
- Super Security Administrator: Creating users, including security administrators and user groups; granting access privileges
- Security Administrator: Creating users, granting access privileges

- Administrator: Creating, editing and deleting user views, screen forms, editing user menu groups and items
- Operator: Working with data accessible to user through user group
- Auditor: Selecting data accessible to user through user group

2 Key Encryption Key Procedures:

2.1 Introduction:

This sets the operational requirements for the generation, custody, exchange and support of a KEK (Zone Master Key).

2.2 KEK Generation/Change Process and Requirements:

- The member must appoint two groups of officers – one shall be responsible for the generation of PIN KEK plaintext parts and the other for the generation of MAC KEK plaintext parts
- The member officers group, also called Member Custodians, under the guidance of SST performs the plaintext KEK parts generation at Switch premises
- The KEK Coordinator at the Member combines KEK parts and confirms Key check value generated at the Switch
- All parties involved in destroying KEK parts

2.3 Key Exchange Key (KEK) Components:

A KEK is composed of 3 components:

- One Member Custodian generates only one component
- The Member Custodians must ensure that all KEK components are generated randomly
- All generation steps are performed for PIN KEK and MAC KEK between the OmanNet and the member bank
- After a KEK is successfully put into production, any unused KEKs shall be destroyed

2.4 KEK Components' Custodians:

- The SST members notify each other of the names of member bank key Custodians and their respective alternates. The alternates should be informed with the absence of the primary Custodians they must assume all of the primary Custodian's duties
- The member bank Custodians must be fully trained and informed of their role as Custodians, they should be aware that they cannot disclose the contents of their respective key component to anyone
- The cryptogram of a KEK, encrypted under a master key, may be maintained by another officer for its implementation in the system database
- In instances where a Custodian cannot perform his or her role, the Member Security Group must authorize a replacement

2.5 Change of Custodian:

- The SST must be immediately notified if a certain form is used upon any change of Custodians. The following steps must be considered:
- The form must be completed entirely upon the change of any Custodian information
- The form will be considered authorized only if the security group at both OmanNet and the member bank signs it

2.6 KEK Generation/Update Procedures:

2.6.1 Within Switch HSM:

Each member bank Custodian will follow all below steps simultaneously

- Member Custodians shall only access the switch HSM under the guidance and control of the SST
- Member bank Custodian will use the HSM to generate a KEK part randomly,
- The Custodian will need to enter:
  - Plaintext KEK part
  - Encrypted KEK part
  - Part check value
- The Member custodian writes plaintext key component with the check value on a special form. This form will be under his custody until delivered to the member bank department responsible for the system
- Encrypted key component is also written by the member bank Custodian on another form. This form is given to the SST. These components are encrypted under OmanNet LMK
- SST will combine these three encrypted KEK components to get the whole KEK encrypted under Switch LMK. The KEK is associated with its check value
- SST writes the whole KEK check value on another form and gives this form to the member bank Custodians

2.6.2 Within Member Bank HSM:

Each member bank Custodian shall follow the below steps simultaneously

- Member bank Custodian encrypts his/her plaintext KEK component under the member bank LMK and confirms the check value generated by his/her HSM with that of OmanNet

- Member bank Custodian fills a form with his/her encrypted component and gives this form to the member bank KEK Coordinator
- The member bank KEK Coordinator combines the three KEK encrypted components to get the whole KEK, encrypted under member bank LMK, associated with its check value
- KEK Coordinator shall confirm the check value with that of the OmanNet

2.7 Duties of the SST at the OmanNet Switch:

The SST has the following responsibilities:

- Controlling the access of the OmanNet HSM
- Controlling and guiding the KEK plaintext components generation process
- Preparing all relevant documentation in advance to ensure process completion
- Receive the encrypted form of the KEK components given by member bank Custodians (forms 4, 5 and 6). These forms must be retained in a confidential and secure manner until the completion of the process
- Combining the three encrypted components to form the whole KEK
- Filling another form (form 7) where the encrypted KEK with its check value exists and keeping it in OmanNet safe custody
- Fills another backup form (form 8) where the encrypted KEK with its check value exists and keeps it in another safe outside the OmanNet premises
- Filling another form (form 9) with only the KEK check value and giving it to the member bank Custodian
- Once combined KEK check value is verified with the member bank, the SST will load the encrypted KEK within the OmanNet system
- With the exception of forms 7 and 8, all forms shall be immediately destroyed
- The following must be ensured for forms 7 and 8:
  - A separate envelope will be used for each form
  - The envelope will be sealed with a proprietary seal, signing over the seal in such a manner that any subsequent tampering may be detected easily
  - Signature over the sealed opening, which is subsequently covered by strong and clear adhesive tape, is an acceptable form of proprietary seal
  - Care should be exercised in choosing the type of envelope so that its contents cannot be seen from the outside

2.8 Duties of the Member Custodians at the Switch:

The member bank Custodians at the Switch have the following responsibilities:

- Generate a 16-character hexadecimal key part using the Switch HSM
- Fill a form (forms 1, 2, 3) with the Plaintext key components and their corresponding check value. These forms must be retained in a secure and confidential manner until the completion of the process
- Receive the form 9 from SST where the KEK check value exists
- The following must be ensured for each form:
  - A separate envelope will be used for each
  - The envelope will be sealed with a proprietary seal, signing over the seal in such a manner that any subsequent tampering may be detected easily
  - Signature over the sealed opening, which is subsequently covered by strong and clear adhesive tape, is an acceptable form of proprietary seal
  - Care should be exercised in choosing the type of envelope so that its contents cannot be seen from the outside

2.9 Duties of the Member Custodians at the member bank:

Member bank Custodians at the member bank shall have the following responsibilities:

- Retain the plaintext Key parts (forms 1, 2, 3) in a confidential and secure manner until confined into the Member HSM
- Access their own HSM to encrypt the plaintext KEK components under their LMK
- Verify the encrypted components check values with those of the switch (OmanNet)
- Fill other forms (10, 11, and 12) with the encrypted KEK components and deliver these forms to the Member KEK Coordinator
- Deliver form 9 to the member KEK Coordinator

2.10 Duties of the KEK Coordinator at the Member:

The Member KEK Coordinator has the following responsibilities:

- Upon receiving the encrypted KEK components forms 10, 11 and 12, the Coordinator combines them through HSM to generate the whole KEK encrypted under member's HSM LMK
- Fills another form (form 13) with the encrypted KEK and its check value. Another form (form 14) is made for backup purposes. As within the Switch, these two forms shall be kept securely in two separate safes with same procedures as listed before
- Verifies the combined check value with that of the Switch
- Once verified, all forms shall be destroyed except for forms 13 and 14

2.11 KEK Change Procedures:

The date for implementing KEK changes is determined as follows:

- After the first KEK generation and loading has taken place, a meeting shall be held to confirm the date of the next time on which the KEK change will occur and this information will be relayed to the security group at both the Switch and the member bank
- The SST will run the KEK change as a project and will ensure that the KEK change responsibilities are assigned to the appropriate officer(s)

2.12 KEK Initialization:

After the KEK generation and loading has taken place at the Physical Security Device, the following procedures shall be considered:

Step	Description	Responsible
1	The assigned SST Member will contact the SST and Member KEK coordinator	SST and Member KEK Coordinator
2	Each party logs off its own interface and stops the other interface	SST and Member KEK Coordinator
3	Enter the new KEK cryptogram	SST and Member KEK Coordinator
4	Activate the other Switch node	SST and Member KEK Coordinator
5	Check for successful Logon and Key change with the Member Bank	SST
6	If not successful, repeat steps 2 to 5 using the back-up cryptogram	SST and Member KEK Coordinator
7	If step 6 is not successful, repeat steps 2 to 5 using the old cryptogram (fall back)	SST and Member KEK Coordinator

The following is a summary of the fallback procedures:

Step	Description	Responsible
1	If the change fails either at the Member Bank or the Switch, a reschedule is made to fulfill this obligation within 30 days at the most. The process must start from the beginning, i.e. new Key Parts must be exchanged	SST
2	A status update of the day on which KEK changes were made is provided to evaluate the results of the change and decide on further action	SST
3	Report results	SST and Member KEK Coordinator

2.13 KEK Forms

Forms 1, 2 and 3 (Filled by Member)

(Insert Form here)

Forms 4, 5 and 6 (Filled by Member)

Key Exchange Key (KEK) Exchange Form No. 4, 5 and 6

(Insert Form here)

Form 7 (Filled by Switch)

Key Exchange Key (KEK) Exchange Form

(Insert Form here)

Form 8 (Backup Copy Filled by Switch)

Key Exchange Key (KEK) Exchange Form

(Insert Form here)

Form 9 (Filled by Switch)

Key Exchange Key (KEK) Exchange Form

(Insert Form here)

Forms 10, 11 and 12 (Filled by Member)

Key Exchange Key (KEK) Exchange Form No. 10, 11 and 12

(Insert Form here)

Form 13 (Filled by Member)

Key Exchange Key (KEK) Exchange Form

(Insert Form here)

Form 14 (Backup Copy Filled by Member)

Key Exchange Key (KEK) Exchange Form

(Insert Form here)

2.14 Notification Forms:

Member Custodians Notification Form [Filled by the Member]

Key Exchange Key (KEK) Change or Zone Master Key (ZMK) Change:

(Insert Form here)

SST KEK Executor Notification Form [Filled by the Switch]

Notification of KEK Executors at the Switch:

(Insert Form here)

Member KEK Executor Notification Form (Filled by the Member)

Notification of KEK Executors at the Member:

(Insert Form here)

3 Message Authentication

3.1 Introduction

In any form of secure message transfer the data authentication and integrity, i.e. the prevention of unauthorized data modification, must to be ensured without introducing unacceptable performance impact. This will be achieved in OmanNet switch system using Message Authentication Code (MAC) techniques.

The Message Authentication Code (MAC) is a checksum derived by applying an authentication algorithm with a secret key to the message. The computation and verification are both done with the same key. The algorithm is effectively Triple DES (3DES) encryption.

3.2 The MAC Process

The MAC is calculated on selected fields of the message. The selected fields are taken in sequence from the start of the message and added together to form the data string that is used for message authentication. The MAC algorithm used is ISO/IEC 9797-1 Algorithm3.

The following are points to note:

- Use the Initial Vector (IV) = Hex '0000 0000 0000 0000'
- The message has to be divisible by eight and treated as data blocks each of size eight bytes
- If the message is not divisible by 8, pad the message by Hex '0000...00' until the message is divisible by 8 (the last block is 8 bytes long)
- On completion of all blocks, the 64 bit result is the Message Authentication Block (MAB)

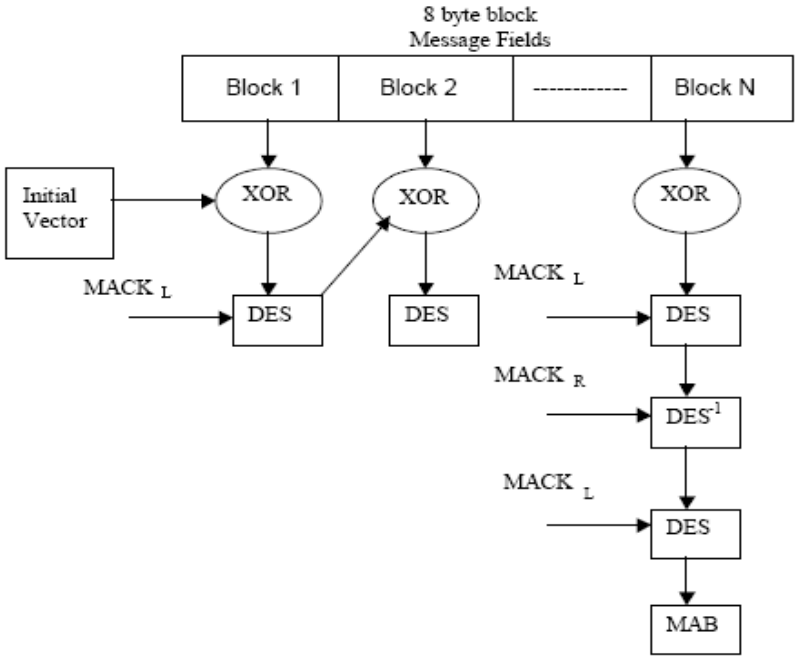

Figure 1- the MAC process

Once the final MAB is obtained, the 64 bits of the field are divided into two halves of 32 bits each. The first 32-bit of the field (Bit 1 – 32) forms the MAC (Message Authentication Code) and is the last data field in the ISO message.

For transactions that utilize only fields in the Primary bit map, Data element 64 will be used to carry the MAC. For transactions than may use both the Primary and Secondary bits maps, the MAC is stored in Data element 128. The second half of the MAB (Bit 33 – 64) forms the MAC Residue.

3.3 Cryptographic Keys Used

For the links between OmanNet and the member banks, a ZAK is used.

3.4 Message Fields to be MACed

Messages exchanged between the OmanNet switch and other parties (member banks, card schemes etc.) as well as between the terminals and the acquiring system must be MACed.

OmanNet will apply the full message authentication mechanism; this means all the data elements of the ISO8583 message will be included when authenticating each external message.

4 Security Incident Resolution Mechanism

4.1 Introduction

Each Member must implement proprietary procedures and processes which form a defensive response to each type of security incident. These processes must also apply to unusual activity which may occur within the service.

The response should be considered in terms of overall cost-effectiveness and prudent management practices.

Member must have a contingency plan to deal with emergency response and fraud detection issues.

4.2 Security Incident Management

4.2.1 Logging Requirements

Logging requirements are provided as follows:

- Each occurrence of a security-related incident must be logged, even in the case of an incorrect PIN
- Logged information must be kept in an access-controlled location for the minimum period specified for record keeping
- Incidents to be logged must include, but are not limited to, the incident types listed below. Security incidents must be accurately identified and reported according to the following categories:
    - Automatically recorded incidents in the Network
    - Incorrect PIN
    - Incorrect MAC values - data used to calculate the MAC is different
    - Invalid PIN Block - ANSI PIN block is incorrect
    - CSM Counter Out-of-Sequence - the message number counter has detected a missing message in the sequence.
    - Message from Unauthorized Terminal - a message has been received from a Terminal which is not authorized by the Acquirer to access the Network.
- A subsequent review of these incidents may be conducted to differentiate true unauthorized messages from, e.g., messages arising from Terminals reported lost or stolen

The above incidents could be caused by:

- Message Authentication failure
- PIN translation/verification errors
- Automated Key distribution errors
- Non-automatic incidents, such as:
  - Any error attending the distribution of manual Keys
  - Known or suspected breach of an ATM
  - Known or suspected compromise of a Key

An incident must remain on record for a period of no less than one year from the date of occurrence.

4.3 Security Incidents Resolution Mechanism

4.3.1 Requirements

The resolution of any security incident may be done on a case-by-case basis provided the Members fulfill the general obligations listed below:

- Each Member Bank must review security incident logs within one Business Day
- Each Member must develop and implement procedures which define the steps for investigating and, where necessary, escalating an incident. Such procedures should include, but not be limited to:
  - Regular follow-up of messages for security incidents. A Member Bank should implement automated techniques as an aid to incident detection and reporting, as well as for alerting the Switch about severe or persistently recurring incidents
  - Guidelines for investigating incidents and for listing causes of error messages according to incident type. Guidelines must include a description of standard methods used for rectifying the problematic Situations
  - Escalation procedures shall allow for the incremental escalation of security-related incidents from the proprietary Network. Contact names, locations and phone numbers to be used in conjunction with the escalation procedures shall be provided to the Switch and shall be maintained updated
  - Member Banks must respond to security incidents with an urgency that corresponds to the severity of the incident(s). In general, prudent business judgment must be used to determine the timing and use of resources for solving any problem. However, a Member must immediately notify the Switch when another Member may be at risk
  - The SST will assist the Switch in resolving security-related incidents

4.4 Fraud Detection and Emergency Response

4.4.1 Escalation Procedures

Member banks must report or escalate to OmanNet any incidents or problems that may affect the network or its members according to the procedures provided in this section.

These incidents can vary in urgency. While certain incidents need prompt action, other incidents are reported only for sharing information with other Members. The Switch in turn will ensure that each incident is acted upon properly.

4.4.2 Types of Incidents

There are three types of incidents:

- Priority "One" incidents that require immediate escalation
- Priority "Two" incidents that are important enough but can wait until the next day
- Priority "Three" incidents that are reported at the next meeting of the Security Committee for the purpose of sharing information with the membership

4.4.2.1 Priority "One" incidents

Description

These incidents are situations whose negative effects such as loss, declines changed to approvals, or bad publicity can still be stopped or minimized if prompt action is taken.

Responding to a Priority "One" Incident

The member bank facing a Priority One incident shall respond in the following manner:

- Complete the Network Form describing the incident and fax it to the Switch Security Team (SST). The transmission of the form should be followed by a phone call to the OmanNet to confirm receipt of the form.
    - The member bank and the SST should immediately discuss the problem
    - The Switch chairman shall be advised of the problem
- The SST will form an emergency team (ET) to solve the problem according to an action plan
- The Switch, its Members and other participants will assume their respective roles according to the action plan
- The SST should ensure that:
    - The ET is following documented procedures
    - The agreed upon action plan is being followed
    - The problem is corrected or, if not, the next plan is being developed
    - Necessary additional steps are identified
    - The SST will hold a follow-up meeting or conference call to report how the problem was handled

- The SST will advise any recommendations for future action based on the response to the problem, and a determination of whether the action plan worked or if another plan should have been adopted

4.4.2.2 Priority" Two" incidents

Description

Priority "Two" incidents are contingencies that can wait until the next day to be resolved.

Responding to a Priority Two Incident

The Member in this situation shall respond in the following manner:

- Complete the Network Form describing the incident and fax the form to the Switch Security Team (SST) as soon as possible but no later than the next day

The SST shall phone the appropriate individuals immediately to set up a conference call to discuss the problem and find out if an ET is needed. The SST will hold a follow-up meeting or conference call to report:

- The SST will hold a follow-up meeting or conference call to report how the problem was handled
- The SST will advise any recommendations for future action based on the response to the problem, and a determination of whether the action plan worked or if another plan should have been adopted

4.4.2.3 Priority "Three" incidents

Description

Priority "Three" incidents are the type of contingencies that do not need immediate or next day attention.

Each Member should have internal procedures and corrective actions allowing it to handle this type of situation. However, these situations will be discussed within the Network Security Committee regular meeting.

Responding to Priority "Three" incidents

The Member in this situation shall respond in the following manner:

- Complete the Network form describing the incident and fax it to the SST
- At the next meeting of the Network Security Committee, the member bank shall raise the problem for discussion
- Member banks may decide to review the matter in-house

4.4.3 Examples

The following tables provide examples of various situations and appropriate responses. In cases where a breach occurs, the network Shared Cash Service breach containment measures require that:

- Affected Members immediately take at least one of the following actions after a Cardholder disputes an ATM cash withdrawal at the branch level:
  - A new PIN is issued or chosen by the Cardholder
  - A new Card is issued (with a new PIN)
- All affected Cardholders shall be advised of the situation and one of the following actions shall be taken:
  - New PIN is issued or chosen by Cardholder
  - New Card is issued (with a new PIN)
  - If duplicate Cards and corresponding PINs are used fraudulently, the only way to stop the ongoing fraud may be to deny further service

4.4.3.1 Priority "One" incidents

Mass Fraud:

Incident	Mass Fraud
Description	Cardholder denies all Transactions; more than one Member is affected
Impact assessment	Major impact: A decision must be made whether to shut down affected nodes and links. The incident may eventually lead to a PIN change by all Cardholders
Involved	All Network Members and SST
Action required	Determine the extent and source of the breach, and then contain it
Proactive action	• Create a prepared statement • Review directive controls • Establish a disaster recovery plan. Review alternative technology plan (Watermark, Smart Card)
Communication method	Arrange for a meeting or conference call

Internal Breach:

Incident	Internal Breach
Description	Internal breach is discovered in one Member. No Cardholders are involved
Impact assessment	Medium impact: A decision must be made whether to shut down affected nodes
Involved	All Network Members and SST
Action required	Disclose the extent of the breach and its probable effect on other Members
Proactive action	Create a prepared statement
Communication method	Conference Telephone calls

Violence to Cardholders:

Incident	Violence to Cardholders
Description	Rash of armed robberies at several Members' ATMs.
Impact assessment	Severe negative impact on consumer confidence in the Member's security set-up.
Involved	SST and various committees.
Action required	Short-term plan to assess and control damage. Long-term solutions should be planned
Proactive action	Create a prepared statement.
Communication method	Conference Telephone calls, face-to-face meetings.

Key Change unsuccessful during node start-up:

Incident	Key Change unsuccessful during node start-up
Description	A node may fail to complete Key exchanges with the Switch because of defective hardware/software, improper startup, table/program object errors, etc.
Impact assessment	Without establishing new Keys, Transactions will be exchanged with old Keys
Involved	SST and affected Members
Action required	See Handling of Exception section.
Proactive action	None.
Communication method	Telephone call.

Site Disaster:

Incident	Site Disaster
Description	Site disaster may be one in which an explosion or fire knocks out part or all of a Member's processing center.
Impact assessment	Severe impact: One or several Members may lose ability to process Transactions.
Involved	Disaster recovery team(s) of the affected Members and the Switch.
Action required	Switch to backup communication lines/backup system.
Proactive action	Notify other Members
Communication method	Conference Telephone call.

4.4.3.2 Priority "Two" incidents

Violence to a Card Holder:

Incident	Violence to a Card Holder
Description	• The Cardholder is assaulted and robbed of wallet and Card while using a Member's ATM • The ATM, located near a parking lot, has no enclosure or security camera that indicates date and time
Impact assessment	Medium impact: Press reports may negatively influence public opinion. This is an isolated incident.
Involved	The Issuer, Acquirer and the SST.
Action required	Block the Card from use, issue new Card to customer.
Proactive action	Create a prepared statement.
Communication method	Telephone Call for the release of a prepared statement to the public and media.

Thresholds exceeded:

Incident	Thresholds exceeded
Description	Security incident thresholds exceeded.
Impact assessment	Medium impact
Involved	Directly affected Members and SST
Action required	Determine the extent of the incident
Proactive action	Look for a pattern of these incidents. Investigate possible causes. Set up meaningful thresholds
Communication method	Conference Telephone calls

Contained Breach:

Incident	Contained Breach
Description	Contained or limited breach. A small number of Cardholders deny making the Transactions in question.
Impact assessment	Medium impact
Involved	All directly affected Members, all other Members and SST
Action required	Find the extent and source of the breach, then customize the prepared statement
Proactive action	Create a prepared statement.
Communication method	Conference Telephone calls.

4.4.3.3 Priority "Three" incidents

Attempted Breach Discovered:

Incident	Attempted Breach Discovered
Description	Attempted breach is discovered before it can be completed.
Impact assessment	Minor impact
Involved	Directly affected Members and SST
Action required	Find out the extent of the situation. Inform the Security Committee at the next meeting. Customize the prepared statement
Proactive action	Create a statement.
Communication method	Security Committee meeting.

Stolen Hardware:

Incident	Stolen Hardware
Description	Hardware such as HSM or ATM is stolen
Impact assessment	Probably minor.
Involved	Directly affected Members and SST
Action required	Report to the SST. The SST should look for patterns and report immediately to its Members any significant activity. The SST should report all incidents at the next Security Committee meeting.
Proactive action	None.
Communication method	Security Committee meeting.

4.5 Response Teams

4.5.1 Switch Security Team (SST)

SST Description

The SST is the group responsible for all security-related issues within the OmanNet switch itself and the zone area between the OmanNet switch and member banks.

The SST provides a forum for assessing problems, which are primarily Priority "One" incidents.

SST Duties

The SST is also responsible for:

- Gathering details of the problem, assessing it and identifying the type
- Determining whether it is necessary to contact directors and how
- Deciding whether an Emergency Team (ET) is required and who shall be a team member of it
- Deciding whether any prepared statements are needed and who should release them
- Spell out the Network's action plan

4.5.2 Emergency Team (ET)

ET Description

The ET should be composed of experts chosen by the SST based on the nature of the incident and affected Members.

ET Duties

The ET is responsible for managing any incident assigned to it by SST as follows:

- Developing and coordinating an action plan for resolving an incident
- Minimizing the incident's negative effects on the Network or its Membership
- Provide regular progress reports to the (SST)
- If required, customize and issue a prepared statement

4.5.3 Switch Security Committee (SSC)

SSC Description

Each Member should have up to three representatives in the Switch Security Committee (SCC). The SCC meets regularly to assess situations of the Switch and its Members.

SSC Duties

The Security Committee shall hold a meeting to:

- Discuss the problem and gather all the details about it
- Set up a meeting for all Members to:
    - Present an assessment of the problem from the point of view of individual Members
    - State their individual approach to the problem
    - Recommend the (SST) action plan
    - Decide if outside experts are needed
    - Establish the frequency of progress reports
    - Arrange other follow-up conference telephone calls or meeting dates to assess the problem on an ongoing basis

4.6 Factors in Determining Severity Level

Factors used in measuring the severity of a problem include the following:

- Type and duration of crisis
- Amount involved
- Number of affected members
- Potential number of affected Cardholders
- Equipment type and configuration involved in the situation
- Affected areas and locations
- Adverse publicity
- Completing the Incident Form

Members that experience an incident must complete the Switch form describing the incident and fax it to the SST. The following information appears on this form:

- Incident Report Number: The Switch assigns this number when it receives the form from the originating Member
- Date Reported: Date when the originating Member completed this form
- Further Information Appended: If the form lacks space and it is necessary to append an information sheet to the form, indicate this by checking YES, otherwise, check NO
- Member originating this report: Name of the Member submitting this form
- For further Information: Name, telephone and fax number of the individual who is most knowledgeable about this incident report
- Date of Occurrence: The date the incident occurred
- Category: The perceived or actual category of this incident, according to the originator
    - This assessment may subsequently be modified as further information becomes available
    - The category may be now “Priority One”, next day “Priority Two” or next meeting “Priority Three”
- Description of Incident: Provides a full description of the incident including its consequences, whether they are confined to one member only or to other members as well
- Impact Assessment: Provides performance degradation caused by this incident
- Resolution: The SST with the Security Committee will provide this information, with details of how it was handled from the beginning to its final settlement