Host Security Module
RG7000

Operations and Installations Manual

1270A513 Issue 3

HOST SECURITY MODULE RG7000
OPERATION AND INSTALLATION MANUAL, REVISION STATUS

Revision	Release Date	HSM Functional Revision
1270A513 Issue 1	January 1999	1.04 / 5.04
1270A513 Issue 2	May 2000	1.05 / 5.05 / Pre-release
1270A513 Issue 3	May 2000	1.05 / 5.05

This manual describes the functionality within the 1.05 and 5.05 base release of HSM firmware for all other versions please refer to appropriate manual and associated HSM firmware specifications.

Zaxus

Europe, Middle East, Africa
Meadow View House
Long Crendon
Aylesbury
Buckinghamshire
HP18 9EQ
UK
Telephone: +44 1844 201800
Fax: +44 1844 208550

Americas
1601 North Harrison Parkway
Sunshine
FL 33323-2899
USA
Telephone: +1 954 846 4700
Fax: +1 954 846 3935

Asia Pacific
Units 2205-06, 22/F.,
Vicwood Plaza,
199 Des Voeux Road, Central,
Hong Kong
Telephone: +852 2815 8633
Fax: +852 2815 8141

HOST SECURITY MODULE RG7000
OPERATION AND INSTALLATION MANUAL

CONTENTS

CHAPTER 1	Introduction
CHAPTER 2	Installation
CHAPTER 3	Configuration
CHAPTER 4	Local Master Keys
CHAPTER 5	Operating Instructions
GLOSSARY	
APPENDIX A	Bisynchronous Connected Option, Programming Examples
APPENDIX B	Asynchronous Connected Option, Programming Examples
APPENDIX C	Channel Attach Option, Configuring the Mainframe
APPENDIX D	SNA-SDLC Connected Option, Programming Examples
APPENDIX E	Standard Visa CW Test Data
APPENDIX F	Warnings, Cautions and Statutory Statements
APPENDIX G	Warranty Statement

CHAPTER 1

INTRODUCTION

CONTENTS

Page

1 GENERAL 1-1

2 HSM FACILITIES 1-3
2.1 KEY MANAGEMENT 1-3
2.1.1 TYPES OF KEYS USED BY THE HSM 1-3
2.1.2 MASTER/SESSION KEY 1-5
2.1.3 TRANSACTION KEY SCHEMES 1-6
2.2 PIN MANAGEMENT 1-17
2.2.1 USER PIN SELECTION 1-17
2.3 MESSAGE AUTHENTICATION CODE 1-18
2.4 CARD VERIFICATION VALUE FUNCTIONS 1-18
2.5 OPTIONAL RSA CRYPTOSYSTEM 1-19
2.6 TRIPLE DES 1-20

3 PHYSICAL DESCRIPTION 1-22
3.1 FRONT PANEL 1-22
3.1.1 FAULT INDICATOR 1-22
3.2 REAR PANEL 1-23
3.3 ELECTRICAL REQUIREMENTS 1-23

4 INTERFACES 1-24
4.1 CONSOLE PORT 1-24
4.2 AUXILIARY PORT 1-24
4.3 HOST PORT 1-25
4.3.1 ASYNCHRONOUS EMULATION 1-25
4.3.2 BISYNCHRONOUS EMULATION 1-26
4.3.3 IBM CHANNEL I/O EMULATION 1-26
4.3.4 SDLC EMULATION 1-26
4.3.5 SNA-SDLC SYNCHRONOUS EMULATION 1-26
4.3.6 ETHERNET 1-26

5 MECHANICAL AND ELECTRICAL SPECIFICATIONS 1-28
5.1 DIMENSIONS 1-28
5.2 DIMENSIONS (CABINET AND 5 UNITS) 1-28
5.3 POWER (PER UNIT) 1-28
5.4 ENVIRONMENTAL 1-28

1 GENERAL

The RG7000 Host Security Module (HSM) series of equipment provides cryptographic functions to support network and point-to-point data security. Acting as a peripheral to a Host computer, the HSM provides the cryptographic facilities required to implement key management, message authentication and Personal Identification Number (PIN) encryption in real time online environments. The HSM is made physically secure by locks, electronic switches and tamper-detection circuits.

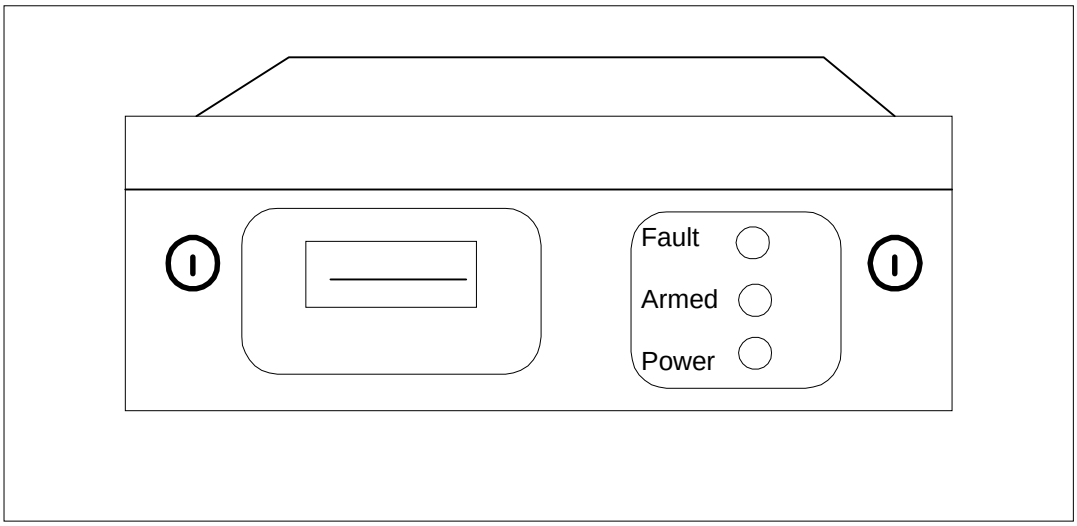


Figure 1.1- RG7000 Host Security Module: General View

The HSM supports a number of standard functions and can be customised to perform client-specific cryptographic functions. Standard functions include:

Verifying and generating Personal Identification Numbers (PINs) such as those used with bank accounts and credit cards.
Generating encrypted card values such as Card Verification Values (CVVs) for the plastic card industry.
PIN solicitation, to obtain a new PIN from a card holder (against a reference number).
Generating keys for use in Electronic Funds Transfer Point Of Sale (EFTPOS) systems.
Key management in non-EFTPOS systems.
Generating and verifying Message Authorization Codes (MACs) for messages transferred via telecommunications networks.

An HSM system consists of up to five units, mounted in a single cabinet, operating independently. A typical five-unit configuration permits concurrent operation for high throughput, and, under control of the application program, provides automatic and immediate backup in the event of a fault in a single unit.

The HSM is normally online to the Host and does not require operator monitoring or intervention. The HSM performs cryptographic processing in response to commands from the Host. The Host sends command messages, which consist of command codes and other fields that are required by the HSM in order to process the commands. The HSM processes the command messages and generates response messages, which also contain a variable number of fields (depending on the message type). Some commands, mainly involving plain text data, are entered by the user via the associated HSM Console.

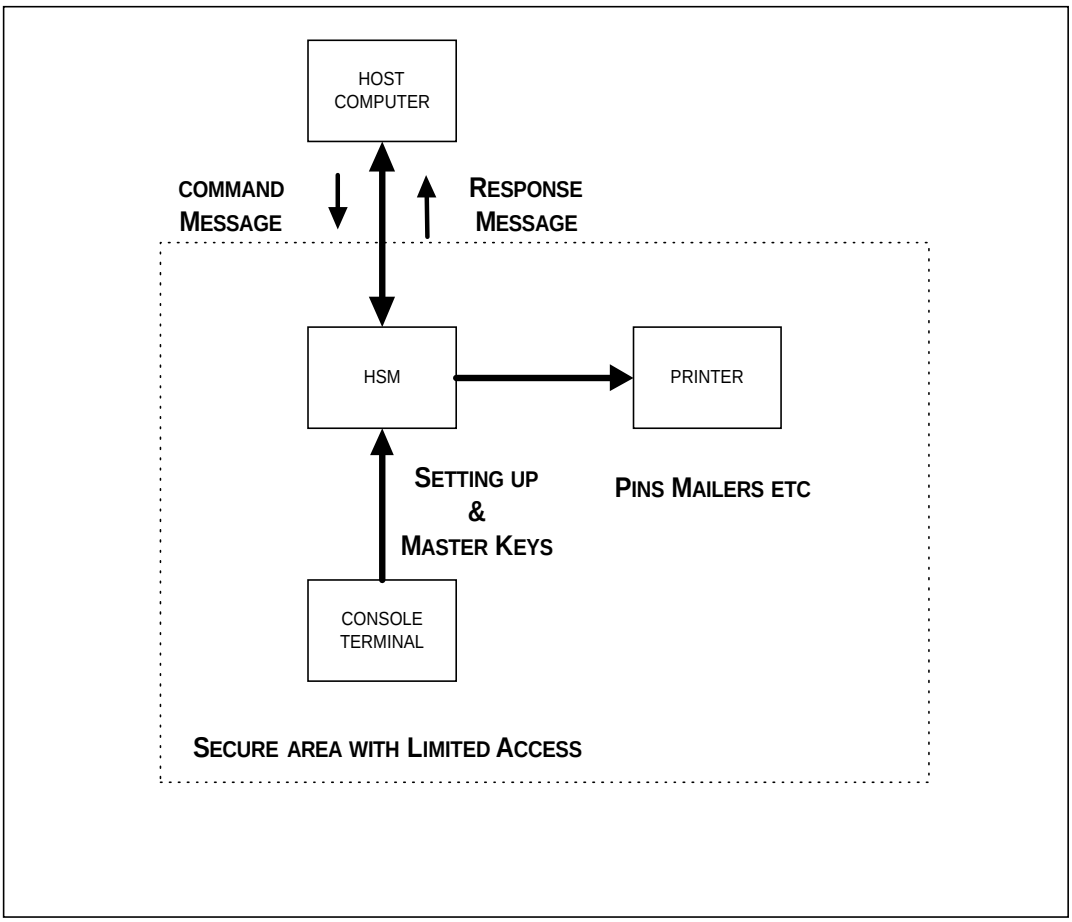


Figure 1.2 - HSM in a Typical System

The throughput of the HSM depends on the types of commands that are executed, and the method and speed of the Host connection.

Note that neither a console terminal nor a printer is supplied with the HSM.

2 HSM FACILITIES

The HSM provides an extensive range of functions including support for key management, PIN generation, encryption and verification, and Message Authentication Code (MAC) generation and verification. It supports standard VISA card operations, with functions for PVV and CVV generation and verification. All commands operate using the Electronic Code Book (ECB) mode of DES unless otherwise stated.

2.1 Key Management

The HSM supports Master/Session Key and Transaction Key management techniques.

Security for key management is ensured by the use of an enforced key hierarchy and the use of multiple Local Master Key (LMK) pairs. The HSM can use Smart Cards (compatible with ISO 7816) to provide a convenient means of handling LMKs.

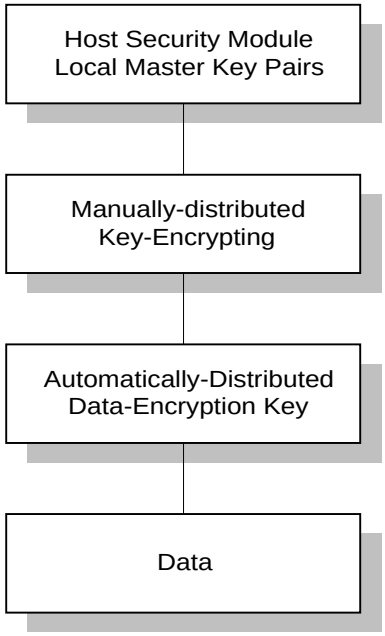


Figure 1.3- Key Hierarchy

2.1.1 Types of Keys Used by the HSM

Local Master Key

The Local Master Keys (LMKs) are a set of Data Encryption Standard (DES) keys stored in the HSM. All other keys and secret data are encrypted under the LMKs for local storage. Up to 20 pairs of LMKs are used with a triple encryption technique which effectively doubles the length of a standard DES key (making it 112 bits long).

For an HSM to operate, the LMKs must be created and loaded. Because the DES algorithm depends on a key for secrecy, and because the security of all keys and data encrypted for storage depend on the LMKs, they must be created and maintained in a secure manner. Provision is made to allow the LMKs to be changed and keys or data encrypted under them to be translated to encryption under the new LMKs.

All keys when stored locally (i.e. not in transit between systems) are encrypted under the LMK.

Zone Master Key

A Zone Master Key (ZMK) is a key-encrypting key which is distributed manually between two (or more) communicating sites, within a shared network, in order that further keys can be exchanged automatically (without the need for manual intervention). The ZMK is used to encrypt keys of a lower level for transmission. For local storage, a ZMK is encrypted under one of the LMK pairs.

Within the VISA environment this is known as a ZCMK.

Zone PIN Key

A Zone PIN Key (ZPK) is a data encrypting key which is distributed automatically and is used to encrypt PINs for transfer between communicating parties (for example, between acquirers and issuers). For transmission, a ZPK is encrypted under a ZMK; for local storage it is encrypted under one of the LMK pairs.

Terminal Master Key

A Terminal Master Key (TMK) is a key-encrypting key which is distributed manually, or automatically under a previously installed TMK. It is used to distribute data-encrypting keys, within a local (non-shared) network, to an ATM or POS terminal or similar. The TMK is used to encrypt other TMKs or keys of a lower level for transmission. For local storage, a TMK is encrypted under one of the LMK pairs.

Terminal PIN Key

A Terminal PIN Key (TPK) is a data-encrypting key which is used to encrypt PINs for transmission, within a local network, between a terminal and the terminal data acquirer. For transmission, a TPK is encrypted under a TMK; for local storage it is encrypted under one of the LMK pairs.

Terminal Authentication Key

A Terminal Authentication Key (TAK) is a data-encrypting key which is used to generate and verify a Message Authentication Code (MAC) when data is transmitted, within a local network, between a terminal and the terminal data acquirer. For transmission, a TAK is encrypted under a TMK or ZMK; for local storage it is encrypted under one of the LMK pairs.

PIN Verification Key

A PIN Verification Key (PVK) is a data-encrypting key which is used to generate and verify PIN verification data and thus verify the authenticity of a PIN. For transmission, a PVK is encrypted under a TMK or under a ZMK; for local storage, it is encrypted under one of the LMK pairs.

Card Verification Key

A Card Verification Key (CVK) is similar to a PIN Verification Key, but for Card information instead of a PIN.

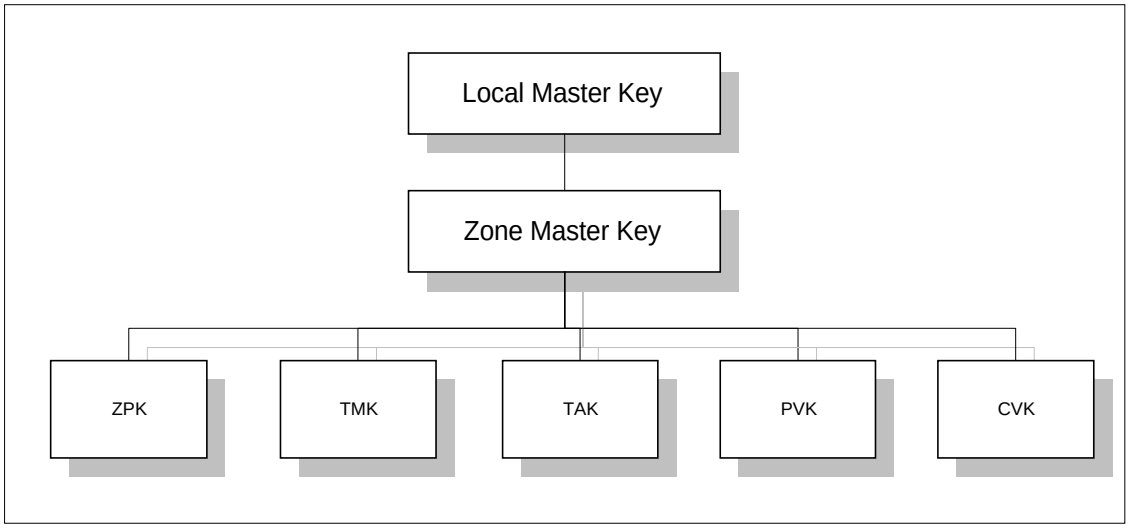


Figure 1.4 - Key Hierarchy for Shared Network Keys

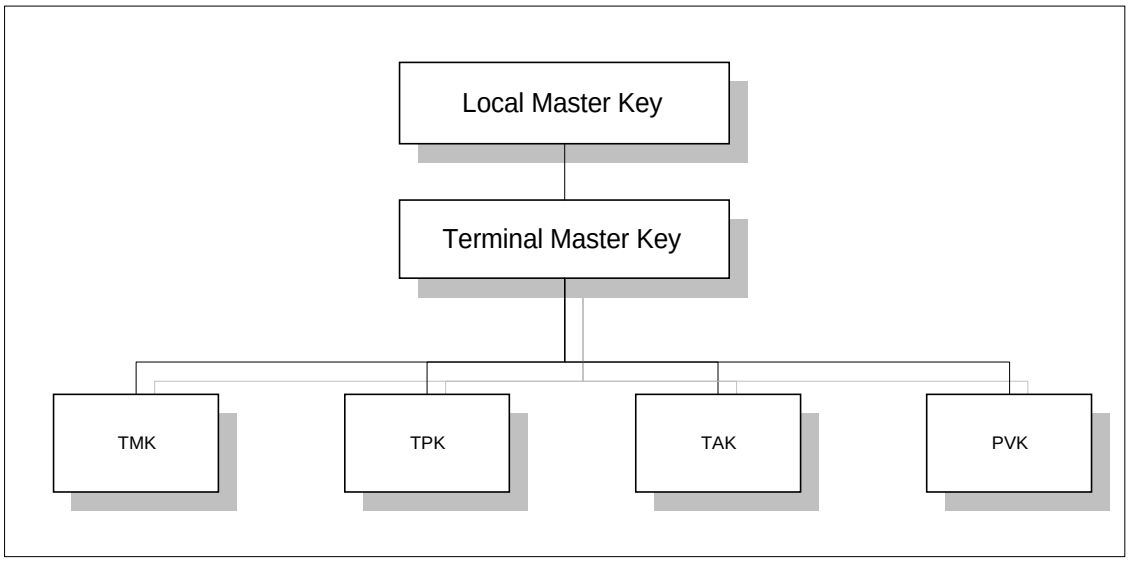


Figure 1.5 - Key Hierarchy for Local Network Keys

2.1.2 Master/Session Key

The master/session key management scheme involves setting up a master key between two communicating parties (for example an acquirer and an issuer or an acquirer and a terminal) under which data-encrypting keys are exchanged for use during a session. Key installation and updating must be organised by the institutions involved (i.e., within the application programs).

The HSM supports master/session key management in both shared and local networks, but distinguishes between the two and maintains separate key hierarchies.

2.1.3 Transaction Key Schemes

The transaction key scheme is a technique in which data-encrypting keys change with each transaction in a manner that cannot be followed by a third party. This is typically of use in Electronic Fund Transfer at Point Of Sale (EFTPOS) systems where fund transfer requests and responses are exchanged between a retailer (EFTPOS terminal) and an acquirer, and then, optionally, between the acquirer and the card issuer.

The HSM supports as standard three techniques "The Racal Transaction Key Scheme (RTKS)", "Australian Transaction Key Scheme (AS2805)" and "Derived Unique Key Per Transaction (DUKPT)".

2.1.3.1 Racal Transaction Key Scheme

In the Racal Transaction Key Scheme the TPK and the TAK are updated after each EFT transaction using an algorithm that depends on the current key and the details of the transaction (which are known to both communicating parties, but which does not form part of the transmitted message, and so would not be known to a third party).

This affords a very high degree of protection for the cryptographic keys. Even if a third party were able to discover the value of the cryptographic key in use at a particular time, this would not facilitate discovery of the keys used on previous transactions (i.e., the scheme has good break-backward protection). Also, if some card data were not transmitted, the third party would not be able to discover the new value of the keys for the subsequent transaction (break-forward protection).

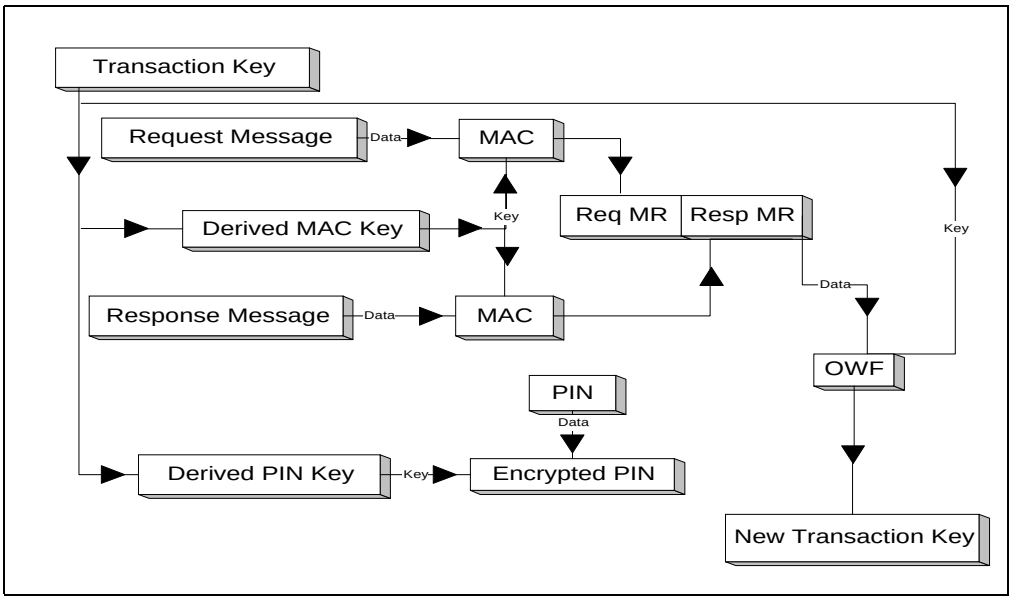


Figure 1.6 - Racal Transaction Key Scheme

The key update algorithm used in the Racal Transaction Key Scheme is based on a one-way function (OWF) involving the current key value and the Message Authentication Code (MAC) residues from the request and response messages from the transaction. The use of the MAC residues is important, as they are not part of the transmitted data.

In this scheme, the MACs are calculated using a key derived from the transaction key, and not the transaction key itself. This also applies to the PIN encrypting key.

For more details of the Racal Transaction Key Scheme see Racal-Transcom Publication RRL4 Secure Key Management for Pin Encryption and Message Authentication.

2.1.3.2 Australian Transaction Key Scheme

The Australian Transaction Key Scheme (ATKS) functions allow Inquirers and Card Issuers to use the HSM and Host computer to perform the security functions defined in Australian Standard (AS) 2805 Parts 4, 6.2, 6.3 and 6.4.

ATKS Support Functions

The HSM is used as a security peripheral on both an Acquirer Host and a Card Issuer Host. It contains a common set of functions; an Acquirer uses a subset of the functions, a Card Issuer uses another subset.

In some applications, an Acquirer can be delegated by the Card Issuer to perform the actual transaction authorization; it is therefore trusted to handle card holder details not otherwise available to an Acquirer. In these applications, both Acquirer and Card Issuer processing are performed on a single HSM.

Acquirer-Only Processing

Acquirer-only processing is used where the Acquirer is also the Card Issuer. The simplified data flow diagram shows the processing that has security implications. When a message is received from the Terminal by the Host, the Host establishes the validity of the message by verifying the MAC (the process depends on whether or not a PIN is in use for the transaction).

The Acquirer Host checks the cardholder's account for availability of funds (no HSM involvement) etc. If a PIN is in use, (sent encrypted from the Terminal to the Host), the HSM uses one of a standard range of verification algorithms to confirm that the PIN is correct.

The Host produces the MAC for the response message to be sent to the Terminal. This includes the Authorization Parameter (Auth Para) if the response message indicates acceptance of the transaction, and excludes it if the transaction is not accepted. (Auth Para is a cryptographically-generated value).

If a cardholder enters an incorrect PIN, the Acquirer returns a "decline" type of response, usually with a request to re-enter the PIN. A re-entry is processed as a new transaction.
The Terminal optionally sends a Completion Confirmation containing a MAC, which the Host checks. The last message, the Completion Response also contains a MAC, generated by the Host.

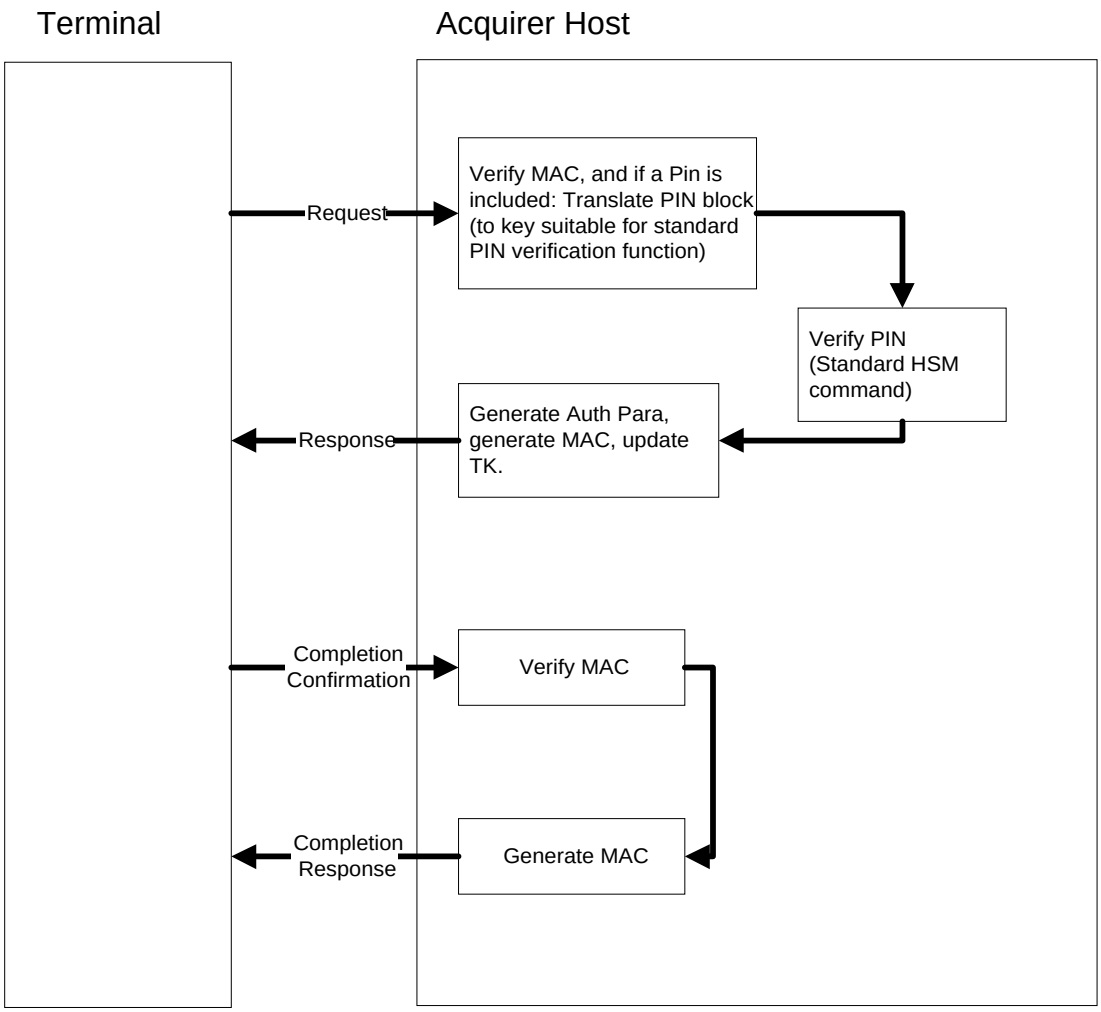


Figure 1.7- Acquirer-Only Processing

Acquirer/Card Issuer Processing

Acquirer/Card Issuer processing is used where the Acquirer is not the Card Issuer. The Request Message MAC verification where no PIN is involved, and the Completion Confirmation/Completion Response MAC processing are the same as in the Acquirer-Only Processing section.

The Acquirer Host performs the Request Message MAC verification and returns the PIN Encrypting Key (PEK) under which the PIN block is encrypted. The PIN block is double encrypted, first by the Card Key, a value not normally available to an Acquirer, then by the PEK. The Acquirer can perform the decryption using the PEK but cannot carry-out the second decryption to reveal the plain PIN block.

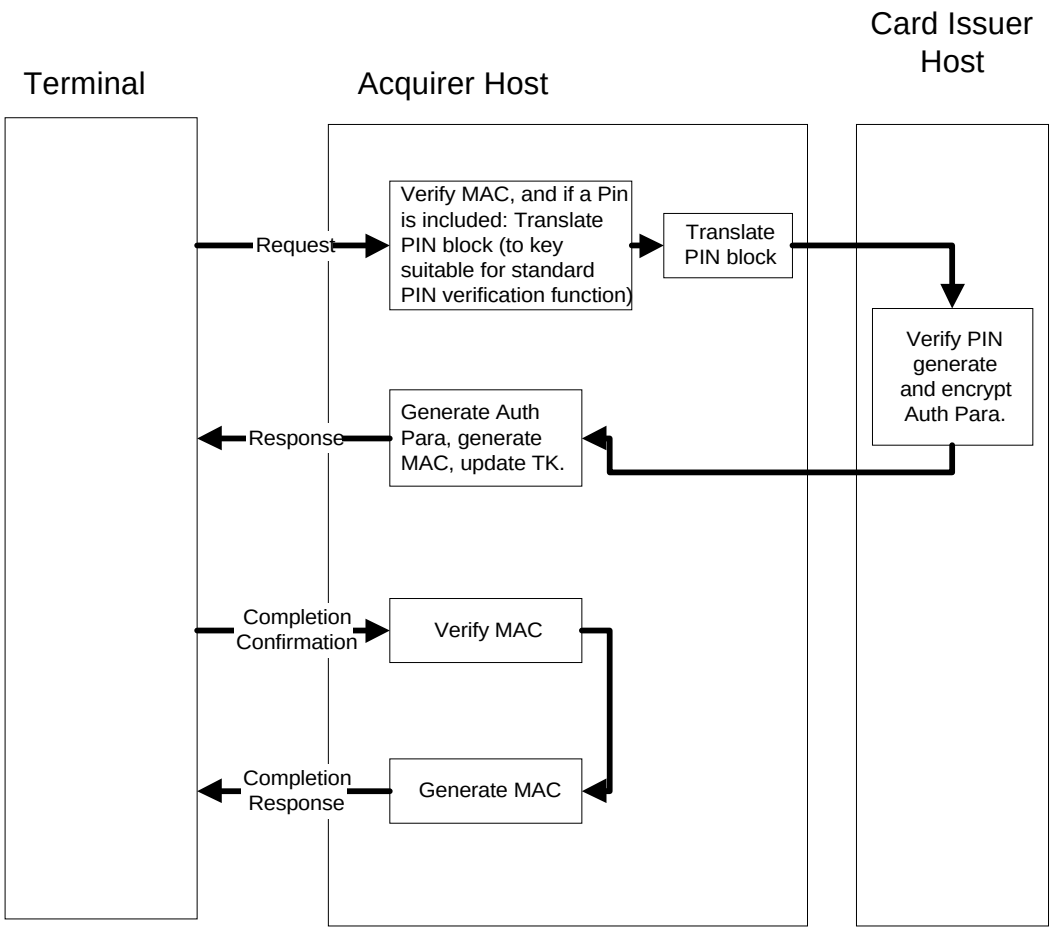


Figure 1.8 Acquirer / Card Issuer Processing

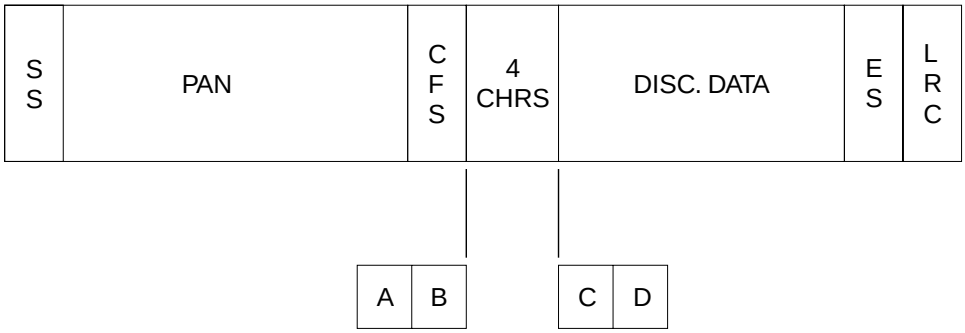
However, the Acquirer can perform a translation so that the PIN block, encrypted under the Card Key, is returned encrypted under a zone ('interchange') key previously set-up between Acquirer and Card Issuer. The translation is a separate function because at the time of message authentication, most software packages are not aware of the ultimate Card Issuer and hence the zone key. This is normally available to the Card Issuer handling part of the software that invokes the translate function.

The last Acquirer function generates the MAC for the outgoing response message. Auth Para, if included, is obtained from the Card Issuer. It is transported to the Acquirer encrypted under a variant of another zone key.

It is assumed that all messages going to and from the Card Issuer are protected by MACs. Two binary MACing functions (not shown in the diagram) are provided for this purpose, using traditional master/session keys: one generates a MAC for a given binary message, the other validates the MAC.

The Card Issuer receives the message containing the encrypted PIN block from the Acquirer Host, and verifies the PIN, using one of the PIN verification algorithms (IBM, Diebold, Visa PVV) or straight comparison. The verification function also generates Auth Para and encrypts it under a variant of a zone key for sending to the Acquirer.
If no PIN has been used with a transaction, a function to generate Auth Para and encrypt it under a variant of a zone key is available.

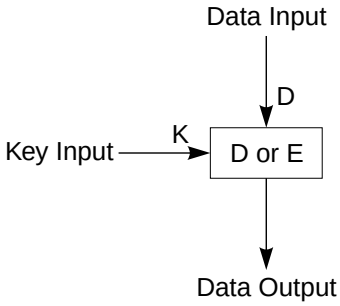
Background InformationFormation of AB and CD Fields from Card Data
The AB and CD fields are derived from the data on the magnetic stripe of the plastic card. There are variations in the way the data is derived. The Acquirer Host and Card Issuer Host systems must match the method implemented on the Terminal. It is the responsibility of the Host to obtain the AB and CD fields and submit them to the HSM in the Host command format. Typically, the fields are derived from an ISO 3554 card as follows:



Where:

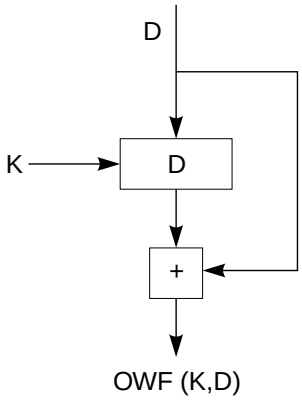
SS	:	Start Sentinel.
PAN	:	Primary Account Number.
CFS	:	Card Field Separator.
4 CHRS	:	Four characters.
DISC.DATA	:	Discretionary Data.
ES	:	End Sentinel.
LRC	:	Longitudinal Redundancy Check.

DEA Encrypt/Decrypt
The basic cryptographic technique is the Data Encryption Algorithm (DEA), defined in AS2805 Part 5. This is the same as the Data Encryption Standard (DES). It is represented as:



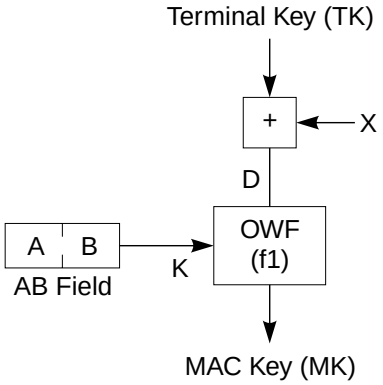
The function can be either an encrypt function denoted by an E in the box or a decrypt function denoted by a D. The key input is 64 bits, of which 8 bits correspond to DEA parity bits and are not used as part of the function.

Function f1, One-Way Function (OWF)
Function f1 takes two 64 bit values K and D and forms an output as follows:



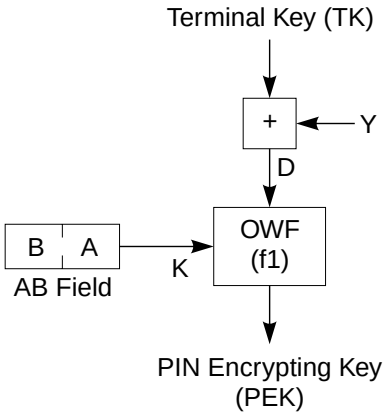
The + signifies a 64 bit exclusive-OR function (modulo 2 addition). For the K input, only 56 bits are used as part of the function, the other eight being DEA parity bits.

Function f2, MAC Key Formation
Function f2 is used to form a MAC Key (MK).



X = 2424242424242424 (16 hexadecimal characters representing 64 bits).
D and K are both 64 bit values, but for K, 8 bits correspond to DEA key parity bits and are not used as part of the process. TK is a 64 bit value without parity adjustment, so parity should NOT be checked when recovering it from encryption under an LMK as all 64 bits are active.

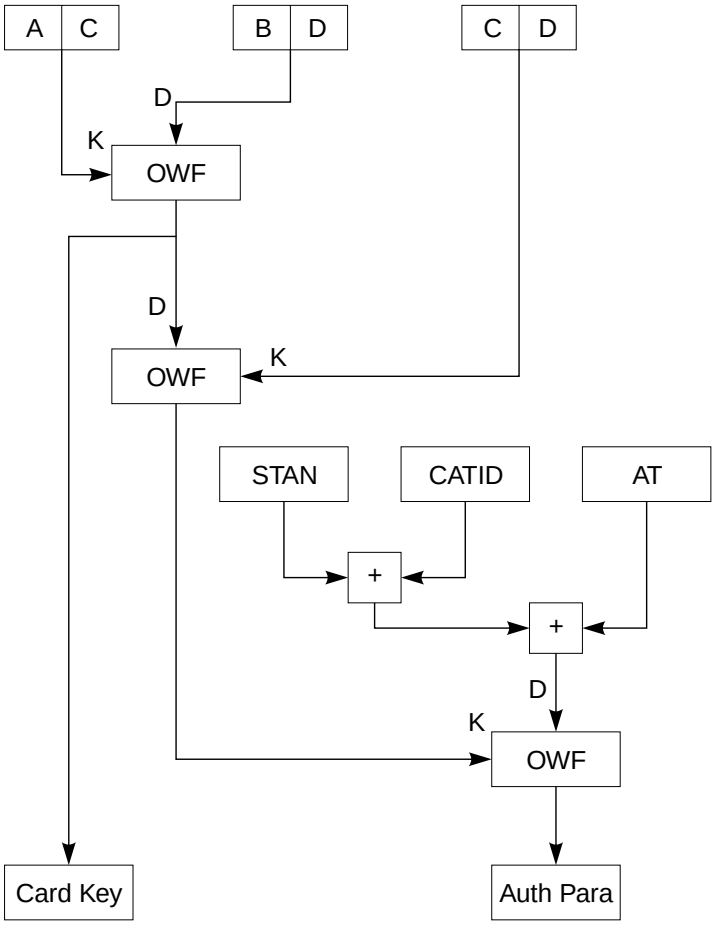
Function f3, PIN Encrypting Key Formation
Function f3 is used to form a PIN Encrypting Key (PEK).



X = 2828282828282828 (16 hexadecimal characters representing 64 bits).
D and K are both 64 bit values, but for K, 8 bits correspond to DEA key parity bits and are discarded. TK is a 64 bit value without parity adjustment, so parity should NOT be checked when recovering it from encryption under an LMK as all 64 bits are active.
The A and B fields are in the reverse order compared with MAC key formation.

Use of HSM User Storage for Keys
The HSM contains an area of memory which can be used for storage of frequently used values such as keys. The use of user storage for Terminal Keys is not recommended because the memory is volatile and not automatically updated.

Generation of Auth Para and Card KeyThe Authorization Parameter (Auth Para) and Card Key are formed as follows:

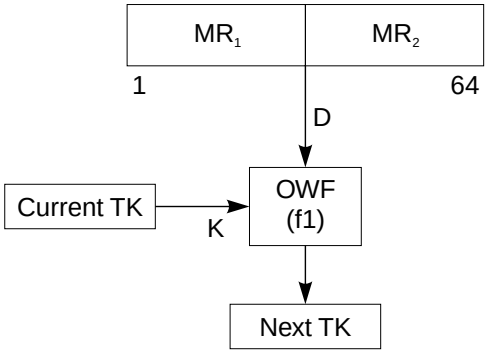


ABCD represent the fields from the card as described in the Formation of AB and CD Fields from Card Data section. The Systems Trace Audit Number (STAN), the Card Acceptor Terminal Identification (CATID) and the Amount Transaction (AT) are values supplied to the generating function. They are combined as follows:

- The 6 digits (24 bits) of STAN are left-justified, right zero-filled to a total of 64 bits, shifted left one bit (with a zero added on the right), and exclusive-OR combined with the 8 characters (64 bits) of CATID shifted left one bit and zero filled.
- The result of (1) is exclusive-OR combined with the 12 digits (48 bits) of AT, right justified, left zero-filled to a total of 64 bits.

The value Card Key is used as data into a One Way Function, therefore all 64 bits are active, so the usual parity adjustment for DEA keys must NOT be performed.

Terminal Key Update
The Terminal Key (TK) is updated at the end of a transaction in readiness for the next transaction. It is updated using the two MAC residues, MR_1 and MR_2 and the One Way Function, f1, as follows:



Parity is NOT adjusted on the next Terminal Key.
It is the responsibility of the application software to maintain on the Host database two Terminal Keys in order to perform re-synchronization in the event of lost messages. Usually these are defined to be the last used (and known to be correct) key, and the next predicted key. Care must be exercised to ensure that the database is updated at the correct point in the transaction.

ATKS Host Commands
The Australian Transaction Key Scheme accesses the following commands via the Host port:

Terminal-to-acquirer requests:

- Transaction request without a PIN. Used to receive a cardholder request message from a terminal with no PIN.
- Transaction request with PIN (T/AQ key). Used to receive a cardholder request message from a terminal with a PIN encrypted under the T/AQ key.
- Transaction request with PIN (T/CI key). Used to receive a request from the terminal when the PIN key cannot be determined by the acquirer.

Acquirer-to-terminal responses:

- Transaction response originating at the acquirer. Used when authorization is generated by the acquirer.
- Transaction response originating at the card issuer. Used when authorization is generated at the card issuer.

Acquirer PIN translation:

- Translate a PIN from encryption under the PEK to encryption under a ZPK.

Acquirer completion:

- Verify completion confirmation message from terminal. Used to verify the MAC on a confirmation message from the terminal.
- Generate completion response.

Card issuer support:

- Verify a PIN from at the card issuer:
- IBM.
- Diebold.
- Visa.
- Comparison.
- Generate authorization at the card issuer.

Binary message authentication:

- Generate a MAC on a binary message.
- Verify a MAC on a binary message.

2.1.3.3 Derived Unique Key Per Transaction

The Derived Unique Key Per Transaction (DUKPT) System of “derived” keys is used in a point-of-sale (POS) environment where any one acquirer can accept transactions from a large number of PIN entry devices.

This technique involves the use of a non-secret “key serial number” and a secret “base derivation key”. On each transaction, the PIN pad uses a unique key based on a previous key and the key serial number, which contains a transaction counter. It encrypts the PIN with this key, then returns both the encrypted PIN and the key serial number to the acquirer. In the HSM the key generated by the PIN pad is “derived”, using the original base derivation key and the key serial number supplied by the PIN pad.

The same base derivation key can be used by thousands of PIN pads because each PIN pad has a unique serial number. Therefore each PIN pad produces a unique key for every transaction and a successful cryptographic attack on one PIN pad will have no effect on any other. The acquirer only has to manage a relatively small number of base derivation keys, and the algorithm to derive a given transaction key is designed in such a way as to require very little overhead in the HSM.

The Host has the responsibility for maintaining the base derivation keys. For each transaction, the Host verifies that the serial number supplied by the PIN pad is valid and extracts from internal storage the appropriate encrypted base derivation key identified by the left-most portion of the serial number. The Host controls base derivation key generation.

This section describes the facilities in the HSM to manage the POS-derived key environment: generating the base derivation keys and online PIN translation and verification transactions.

Key Serial Number
The Key Serial Number (KSN) is a variable-length hexadecimal value which uniquely identifies each PIN pad. This number consists of several fields, as follows:

- Base derivation key identifier (mandatory): five to nine hexadecimal characters.
- Sub-key identifier (optional): reserved for future use. Currently set to zero.
- Device identifier (mandatory), used to ensure that this key serial number is unique: two to five hexadecimal digits. **No two PIN pads with the same base derivation key and sub-key identifiers may be given the same device identifier.** Because the PIN pad packs the left-most bit of the transaction counter as the right-most bit of the device identifier, this field is always even (the right-most bit is set to zero).
- Transaction counter supplied by the PIN pad to identify a particular transaction: 21 bits. Used by the HSM to compute the actual PIN key. The left-most bit is supplied as the right-most bit of the device identifier.

The PIN pad cannot accept a serial number longer than 20 characters, so the Host ensures that the total length of the first three fields does not exceed 15 characters.
The Host also supplies to the HSM a three-character KSN descriptor, which defines the length of each field in characters. It is included with the KSN in Host storage, and is used by the Host to identify the base derivation key. The KSN descriptor consists of:

- Left character: base derivation key identifier length.
- Middle character: sub-key identifier key length (0 if no sub-key is defined).
- Right character: device identifier length.

Zone Master Key (ZMK) Support
The HSM supports single-length Zone Master Keys (ZMKs), 16 hexadecimal characters (64 bits); and double-length Zone Master Keys (*ZMKs), 32 hexadecimal characters (128 bits). (A double-length key is indicated by an asterisk (*) preceding the key type). The DUKPT command set ignores the S/D (single/double length) parameter set by the CS (Configure Security) command.

Base Derivation Key (*BDK) Support
Base Derivation Keys (*BDKs) are double-length keys. There are three Host transactions to generate and translate *BDKs. The BI command generates a random *BDK and returns it to the Host encrypted under Local Master Key (LMK) pair 28-29. The DW command accepts a *BDK encrypted under a Zone Master Key (*ZMK) and translates it to LMK pair 28-29. The DY command translates a *BDK from LMK to *ZMK encryption.

Host Pin Translation and Verification
The HSM performs two functions for the Host communicating with POS terminals:

- It translates a PIN from encryption under the base derivation key to encryption under the appropriate interchange key shared between the acquirer and the issuer or switch.
- It verifies the PINs received from a terminal using base derivation keys. All four HSM verification methods (IBM, Diebold, VISA PVV and Encrypted PIN) are supported.

2.2 PIN Management

A typical example of a PIN used to validate a financial transaction is as follows:

The card issuer generates a unique PIN for the account holder (it may also be unique for each card held by the account holder), in accordance with a defined algorithm. A value known as an 'Offset' can be stored on the card.

The cardholder enters the card at an Automated Teller Machine (ATM), and enters the PIN at a keypad.

The ATM forms a PIN block from the account number and the entered PIN, and encrypts it under the TPK. The encrypted PIN block is sent to the acquirer.

The acquirer translates the PIN block from encryption under the TPK to encryption under the ZPK to send to the card issuer. While in plain text (inside the HSM), a different PIN block format can be created, as agreed between the acquirer and card issuer. The new encrypted PIN block is sent to the card issuer.

The card issuer supplies the encrypted PIN block with some other data to the HSM, which verifies that the PIN is correct for this account (or card), according to the algorithm.

To support PIN transactions, the HSM provides a range of PIN management functions including:

- PIN Generation.
- PIN Block Translation.
- PIN Verification.

2.2.1 User PIN Selection

A PIN can be selected by the cardholder in an online environment, depending on the type of algorithm and whether the card can be written-on by the ATM (or similar); or, using a manual selection technique on a form known as a "PIN Solicitation Mailer".

A solicitation mailer is a turnaround form which is sent to the cardholder. The cardholder records the PIN selection on the form and returns it to the issuer. The mailer data consists of the cardholder name and address, and a reference number (an encrypted account number). As a security measure, the form returned to the issuer contains only the reference number and the PIN selection.

2.3 Message Authentication Code

The Message Authentication Code (MAC) can be computed to verify that a message transferred by a telecommunications network has not been altered. This method involves submitting sensitive elements of a message to DES with a secret key.

The originator appends the MAC to the message. The recipient uses the same elements and secret key to compute the MAC and compares it with the one sent by the originator. If the two agree, the message is accepted as valid.

The user chooses several parameters:

- Which fields to use in the MAC computation, the order of the fields, their format, and any editing criteria.
- Character coding (for example, whether or not data is represented in ASCII or EBCDIC).
- DES key management: although not part of DES, secure key storage and transmission are vital to the integrity of the MAC.

HSM transactions assume:

- The Host computer is responsible for all data editing. The HSM is supplied with a variable-length data field for MAC computation, and except for zero filling of the last 64-bit block, uses all supplied data in the order provided.
- All MACs are computed on ASCII data (EBCDIC data is converted to ASCII before computation).

2.4 Card Verification Value Functions

The Card Verification Value (CVV) is a cryptographic check value derived from specific fields of data, such as account number, card expiration date, service code, and keys (CVKs).

The CVV is written onto the card. During transactions it is sent to the HSM which recalculates the CVV and compares it with the received CVV to confirm the validity of the card.

2.5 Optional RSA Cryptosystem

Introduction
The RSA public key algorithm was devised in 1979 by Rivest, Shamir and Adleman (hence the name). It is an asymmetric cryptographic algorithm, which means that the encryption and decryption keys are different, and that it is computationally infeasible to deduce the decryption key from the encryption key. The encryption key may be made public and distributed in clear without compromising the security of the decryption key, hence the term Public Key Cryptography.

RSA public-key cryptography is usually used in two ways:

- To digitally sign electronic messages to provide proof of the identity of the sender, and to protect the integrity of the contents of the messages.
- To automate and simplify the difficult problem of secret key distribution and management in large distributed networks, such as the Internet.

The RSA algorithm is implemented in a Digital Signal Processor (DSP) which fits inside the HSM on a daughter board. Two versions of the board are available: one has a single DSP processor, the other has two DSP processors, the second a slave to the first. The single-DSP board is used in the Standard HSM range to provide RSA functionality; the double-DSP board is used in the High-Speed HSM range to provide high-performance RSA processing.

Functions are provided for:

- Generation of variable-length RSA keys.
- Validation of public key certificates.
- Generation and validation of digital signatures.
- Secure DES key management using RSA public master keys.
- Generation of hash values.

To conform to international export controls, no functions are provided for straightforward RSA data encryption and decryption.
The length of the RSA keys used can be selected from 320 to 2048 bits for signature functions, and from 320 to 1024 bits for DES key management functions.

HSM Buffer Sizes
The High-Speed HSM has a 32K-byte input buffer; the Standard HSM has a 2K-byte buffer. It is the responsibility of the host application to ensure that that the total amount of data sent in an HSM command does not cause a buffer overflow.

Data Formats
Certificates, signatures, encrypted key blocks and message data supplied in commands specified in this document are binary fields, with the leftmost byte being the most significant and the rightmost byte being the least significant. Note that the binary data may be right justified and padded to the left with zeros, if necessary, in order to make the data length (in bits) an exact multiple of eight.

Even Public Exponent
There is a variant of RSA (known as the “Rabin” variant) which utilises an even Public Exponent. This variant cannot be used for unique encryption/decryption unless the associated data contains some redundant information which can be used to determine the correct result. Although the commands specified in this document, which use a Public Key, could be used with an even Exponent, there is no guarantee that the results produced by these commands will be correct. It is strongly recommended that the commands in this document are used only with odd Public Exponents. Note that it is not possible to use the HSM to generate an RSA Key Set that has an even Public Exponent (see “Generate an RSA Key Set”).

2.6 Triple DES

With the increase in computer processing power an attack on single length DES keys is becoming feasible. This is causing a migration from single length DES keys to double or triple length DES keys.

The HSM supports single, double and triple length DES keys within its command set. If a single length DES key is presented a single encrypt or decrypt is performed. If a double length DES key is presented the processing for encryption is to encrypt using the left key, decrypt using the right key and encrypt using the left key, the reverse is true for decryption. If a triple length DES key is presented the processing for encryption is to encrypt using the first key, decrypt using the second key and encrypt using the third key, the reverse is true for decryption. This supports the standard ANSI X9.52 mode when operating Triple DES

The HSM console or host commands recognise the key length by considering the first character of the presented key:

If the first character of the key is a hexadecimal character (0 – 9 or A – F) this is considered to be the first character of a single length DES key.
If the ZMK has been configured as double length and for some specific keys this is considered to be the first character of a double length DES key.
If the first character is "K" or "S" this is an index to user / secure storage and a single length DES key is extracted.
These modes are required for backwards compatibility.

If the first character is not a hexadecimal character or "K" or "S" this is a key scheme tag and defines the key length and encryption scheme used the key follows the tag. Key schemes tags come in pairs one for double length DES keys and one for triple length DES keys. When a key scheme is used the encrypting key must be the Local Master Key or a double / triple length key for import / export.

There are currently two key schemes defined:

ANSI X9.17 method
Each key of a double or triple length key is encrypted separately using the ECB mode of encryption. This scheme is only available for import and export of keys and must be enabled via the Configure Security (CS) command.

The tags for this scheme are as follows:
X – Double length DES keys
Y – Triple length DES keys.

Variant method
Each key of a double or triple length key is encrypted separately using the ECB mode of encryption. For the second or third key, depending on whether it is a double or triple length key, a variant is applied to the encryption key. There are five variants to enable the encryption of each key distinctly. This application of variants enforces the key use as a double or triple length key and the key order. This scheme is available for encryption of keys under the Local Master Key and for import and export of keys.

The tags for this scheme are as follows:
U – Double length DES keys.
T – Triple length DES keys.

The Variants applied are as follows:

Double length key	Key 1 of 2 – A6
	Key 2 of 2 – 5A

Triple length key	Key 1 of 3 – 6A Key 2 of 3 – DE Key 3 of 3 – 2B

3 PHYSICAL DESCRIPTION

An HSM system consists of up to five HSM units in a cabinet (with blanking plates if fewer than five units are fitted). The front panel of each unit is accessible from the front of the cabinet. The rear of the cabinet has a lockable door which gives access to the rear panel of each unit. The units are supported on telescopic runners so that they can slide out via the front of the cabinet.

3.1 Front Panel

The hinged front panel (see Figure 1.1) is secured by two cam locks. An HSM can be opened only when the two authorised key holders are present. After installation, it is not necessary to open the unit unless it requires maintenance (except to change the Local Master Keys (LMKs)).

The ARMED indicator on the front panel illuminates when the tamper-detection circuit is armed (i.e., set ready to operate), the POWER indicator illuminates when power is applied, and the FAULT indicator illuminates when there is a fault.

The Smart Card reader is an ISO card compliant type with automatic card ejection. The card is ejected at standard points in HSM operation:

- On completion of a Smart Card related Console command.
- Following premature Console command termination when the user presses the <Delete> key or the CTRL-C key combination.
- When the HSM is reset by the RESET button on its rear panel.
- During diagnostic testing.

3.1.1 FAULT Indicator

The FAULT indicator is normally extinguished. If the automatic self checks that occur at power-on and reset are not successful, the FAULT indicator either illuminates continuously to indicate that the unit has failed and should not be used, or it flashes to indicate that the unit may fail in the near future.

FAULT Indicator	Fault	Recommended Action
Continuously illuminated	Program memory (PROM) or working memory (RAM) has failed power-on test.	Reset HSM or switch power off then on. If the indicator remains illuminated there is a fatal error.
Flashing	Non-volatile memory support battery voltage is low.	Run diagnostic test (Console DT command) to validate fault. Check battery jumper is fitted.
Flashing	Crypto-processor failure.	Run diagnostic test (Console DT command) to validate fault.

3.2 Rear Panel

The power input (via an IEC connector), voltage selector and fuse (20 mm type) are housed in a module in the lower left hand corner (see Figure 1.9).

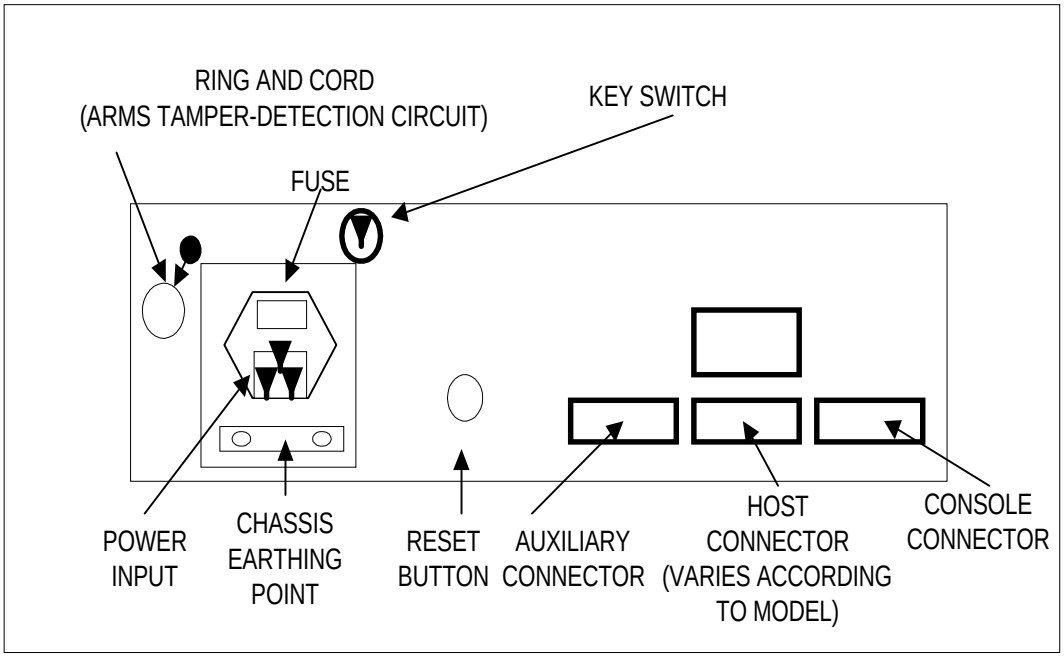


Figure 1.9 - RG7000 RearView

The Console port, Host port and Auxiliary port are 25-way, D-type sockets with screw fixings. Channel connect versions have four large bus and tag connectors as alternative connections for the Host port.

The KEY switch is operated at unit installation, during the generation and installation of the LMKs, or to allow some diagnostic functions.

The tamper-detection circuit is armed by a ring and cord: when the ring is pulled, it activates the detection circuitry, and pushing the ring cannot de-activate it. The ARMED indicator on the front panel illuminates when the ring has been pulled.

3.3 Electrical Requirements

All electrical connections are made at the rear panel of the HSM. HSMs are independent and each HSM in a cabinet requires power (115/230 volts) and connection to a Host port. If the Host computer runs from an uninterruptable power supply, connect the HSM to the same supply.

A chassis earthing point is fitted to provide a good electrical connection, via a substantial braid, to a low impedance building earth, which may be required for compliance with safety or EMC regulations.

4 INTERFACES

The HSM receives command messages via the Host interface. A message contains all the data required by the HSM to perform a cryptographic operation. The HSM processes the data, and generates a response message which it sends to the Host. If the HSM identifies errors in the received data, it sends an error code.

A Console (and optionally a printer) are used to perform tasks involving plain text keys or PINs, set the HSM into the Authorised state and perform diagnostic functions.

4.1 Console Port

The Console port is configured as a DCE. Almost any asynchronous ASCII terminal is suitable for use with the HSM. The default settings can be chosen to be either 300 baud, seven data bits, odd parity and one stop bit, or 19200 baud, eight data bits, no parity and one stop bit. When the Console is operational, the baud rates and word formats can be changed to any convenient value.

Console operations include generating and loading the LMKs and Passwords, setting the HSM into the Authorized state by using the two Passwords or Smart Cards and PINs, generating manually-distributed master keys and performing diagnostic functions. The terminal must therefore be located in a secure access-controlled area.

The console terminal is not required all the time therefore it is possible to share a terminal across a set of HSMs. The use of a RS232 switch box may make this easier.

4.2 Auxiliary Port

A printer is required to print PIN mailers or generate and print components of manually-distributed keys. It must support serial data communications and is connected to the HSM via the Auxiliary port.

In normal operation, the HSM is set into the Authorized state by the use of the Console, then printing can start. The printer must be located in a secure access-controlled area.

4.3 Host Port

The Host port can be programmed from the Console to provide a number of different emulations, according to the type of HSM.

HSM Type	Emulation						
	Async	Bisync	SDLC	SNA/SDLC		FIPS-60	TCP/IP
	RS-232	RS-232	RS-449	RS-232	V.35	IBM Channel	Ethernet
RG7100 / RG7110	✓						✓
RG7200 / RG7210						✓	
RG7300 / RG7310	✓	✓	✓				
RG7400	✓	✓					
RG7500	✓			✓			
RG7600	✓			✓	✓		

4.3.1 Asynchronous Emulation

4.3.1.1 Standard Asynchronous Emulation

Asynchronous emulation is half duplex, the Host must receive the response from the HSM before sending another command. There is no inherent flow control; the HSM returns its response as soon as it has finished processing a command. Typical processing times for PIN translations and verifications are 50 to 70 milliseconds. If the Host is logically half duplex and cannot receive such a quick response, a preset delay of 1 to 255 milliseconds can be inserted before the HSM sends the response.

Each command message to the HSM starts with STX (hexadecimal 02) and ends with ETX (hexadecimal 03). The response to the Host is also bracketed with the STX/ETX pair. These characters are the only data link control codes recognised, and any data between an ETX and the next STX is discarded. The HSM can be programmed to replace the ETX in its response with a one or two character string selected by the user, but the data from the Host is always terminated by ETX.

The data in the Host commands and the HSM responses is always ASCII character data. Raw binary data is never sent; keys and PIN blocks are converted to their hexadecimal character representations (0-9, A-F) for transmission.

4.3.1.2 Transparent Asynchronous Emulation

In order to send binary data, the HSM can be configured for transparent asynchronous communications, in which it sends STX then the count (number of bytes), the data, a redundancy check character and ETX. The receiving unit verifies the redundancy check (which is over just the data), and confirms the number of bytes before accepting the data.

4.3.2 Bisynchronous Emulation

The HSM can be programmed to emulate an IBM 3270 control unit. It appears as a 3271 Model 1 Cluster Control Unit with one 3277 Terminal attached; however, the emulation is sufficiently general for almost any 3271, 3274 or 3276 configuration to be used.

The data protocol conforms to the IBM 3270 multipoint bisync standard. Host command messages to the HSM may contain binary data provided the blocks of data are correctly delimited by the DLE character (X'10) as specified in the 3270 protocol. However, the data in the HSM response is always character data. In the normal (character) mode of operation, keys and PIN blocks are converted to their hexadecimal character representations for transmission. For more information, see IBM documents GA27-3004 and GA27-0060.

Options include selecting the character set (EBCDIC or ASCII), specifying the poll and select addresses, special support for the CICS and IMS environments, and defining the electrical interface to be either a DCE or a DTE. The latter is useful if multiple ports are not available on the communications controller: the five HSM units can be configured to look like terminals, and a Port Sharing Unit/Modem Eliminator can multiplex all five into one 3705/3725 port. Note, however, that use of a Port Sharing Unit degrades the optimum performance available from a set of HSMs because they are all connected to the same communication line.

4.3.3 IBM Channel I/O Emulation

The channel attach option emulates a basic tape control unit with limited command capabilities and can connect to any computer byte or block multiplexer channel meeting IBM specification GA22-6974-6. It can also interface to any plug-compatible equivalent channel that conforms to the NBS FIPS-60 specification. Manufacturers include Amdahl, Camdex, CDC Omega, Cray, IPL Systems Magnuson, NAS, Nixdorf, NCR and Sperry-Univac. The IBM range includes 360, 370, 4300 series, 3080 series and the 3090 series.

4.3.4 SDLC Emulation

An HSM is viewed by the Host as a DCE (data communications equipment) operating as a non-switched point-to-point half duplex device; the electrical interface conforms to the RS-449 standard without the secondary channel. An HSM configured for SDLC has a number of user-configurable options; these parameters should be defined before configuring the unit.

Options include selecting the character set (EBCDIC or ASCII), the message header length (from 1 to 255 characters), the station address and the baud rate.

4.3.5 SNA-SDLC Synchronous Emulation

The SNA-SDLC interface provided in the HSM emulates a 3274 Control Unit (CU) with a single device attached. At the SNA level this Control Unit appears as two Network Addressable Units (NAU); a Physical Unit (PU) and a Logical Unit (LU). (A standard 3274 CU contains 32 such LUs.) The electrical interface between the Host and the HSM conforms to either the RS-232C standard or the V.35 standard.

Options include selecting the message header length (1 to 100 characters), a Transparent Data mode, operation as a DCE or a DTE, the SDLC Station Address baud rate (if DCE), and the HSM can support the IBM IMS and CICS environments.

4.3.6 Ethernet

The Ethernet interface uses TCP/IP protocol for 10Mbps transmission over shielded coaxial cable, with CSMA/CD as the access control method. The HSM supports two Ethernet interfaces: 10base5 (always active) and 10base2 (selectable); only one can be used at a time.

The HSM acts as a TCP/UDP server supporting connections to up to eight TCP ports or sockets and one UDP port or socket. Applications establish connections to the HSM's ports by first connecting to the Well-Known-Port at the IP address. The Port Number and IP Address are defined for the HSM at configuration.

When the HSM receives a TCP connection request on the Well-Known-Port, it assigns one of the available TCP ports (or sockets) to the session. The original connection to the Well-Known-Port is dropped and all subsequent communication continues with the assigned port. The HSM keeps a count of the unassigned ports, and when there are no free ports available, refuses any additional set-up requests until a port becomes free.

5 MECHANICAL AND ELECTRICAL SPECIFICATIONS

5.1 Dimensions

Height	:	133 mm (5.25 in).
Width	:	483 mm (19 in).
Depth	:	489 mm (19 in).
Weight	:	18 kg (41 lb.).

5.2 Dimensions (Cabinet and 5 Units)

Height	:	740 mm (29 in).
Width	:	510 mm (20 in).
Depth	:	640 mm (25 in).
Weight	:	121 kg (267 lb.).

5.3 Power (per Unit)

Voltage	:	90 to 132 V and 175 to 264 V ranges, auto-selected.
Frequency	:	47 to 63 Hz.
Fuse Rating:		
(115/230 Volt)	:	1.6 A (delayed action).
Consumption	:	50 W (maximum).
Rating	:	50 VA.

5.4 Environmental

Temperature	:	10 to 40° C.
Humidity	:	10 to 90% (non condensing).
Heat Output	:	Less than 50 W total

CHAPTER 2

INSTALLATION

CONTENTS

		Page
1	GENERAL	2-1
2	INSTALLING THE HSM UNITS AND CABINET	2-1
2.1	POSITIONING THE CABINET AND CABLES	2-1
2.2	FITTING THE HSM INTO THE CABINET	2-2
2.2.1	CAM LOCKS	2-2
2.2.2	FITTING THE HSMS TO THE SLIDING RUNNERS	2-2
2.3	OPENING AND CLOSING THE HSM	2-3
2.4	POWER SUPPLY AND FUSES	2-3
2.4.1	CHANGING THE MAINS FUSE	2-3
2.5	PREPARING THE HSM FOR USE	2-4
2.5.1	CONNECTING POWER	2-4
2.5.2	COLD START	2-4
2.5.3	CONNECTING THE BATTERY	2-4
3	CONNECTING TO THE CONSOLE TERMINAL	2-5
3.1	CONSOLE SPECIFICATION	2-5
3.2	CONSOLE AND AUXILIARY PORT INTERFACE SIGNALS	2-6
3.3	CONFIRMING CORRECT CONSOLE CONFIGURATION	2-6
4	CONNECTING TO THE PRINTER	2-7
4.1	PRINTER SPECIFICATION	2-7
5	CONNECTING TO THE HOST	2-8
5.1	HOST PORT CONNECTIONS FOR ASYNC, BISYNC AND SNA-SDLC/RS232	2-8
5.2	HOST PORT CONNECTIONS FOR SDLC/RS-449	2-9
5.3	HOST PORT CONNECTIONS FOR SNA-SDLC/V.35	2-10

1 GENERAL

This chapter describes the physical installation of the HSM in the computer room. It then requires configuration and Local Master Key loading, as described in Chapters 3 and 4.

2 INSTALLING THE HSM UNITS AND CABINET

An HSM system consists of up to five HSM Units in an optional cabinet (see Figure 2.1), which should be installed as a peripheral device in a computer room. The maximum recommended ambient temperature for operating HSMs is 40°C. Consideration must be made to the airflow and temperature when the units are installed in a cabinet so to ensure this temperature is not exceeded. Additional cabinets and units may be added as needed

The equipment is delivered in a number of boxes, one for the cabinet and one for each HSM unit with its power cables.

A set of blank Smart Cards is normally shipped with one of the HSMs, and a set of physical keys is supplied with each HSM unit. The keys are sometimes taken to the installation site by an installation engineer.

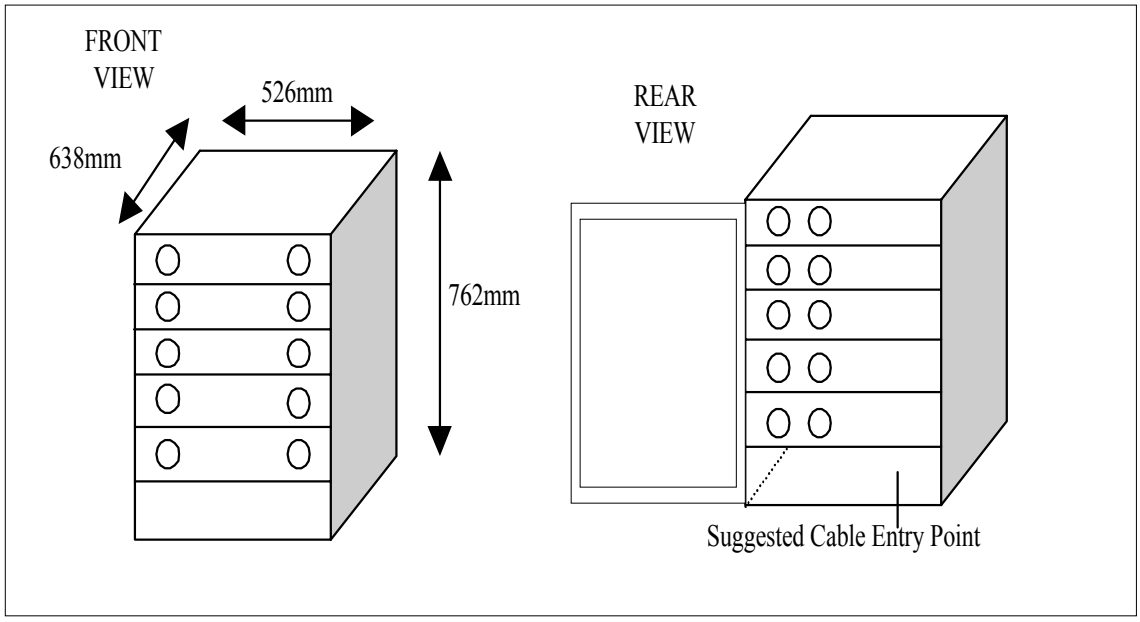


Figure 2.1- Typical 5-Unit Cabinet

2.1 Positioning the Cabinet and Cables

Access is required to the front and the rear of the cabinet, about 1220mm (4ft) in each case. The cabinet has no base so, if the computer room has a raised floor, cables can be passed up to each HSM, from under the rear left-hand corner (as shown in Figure 2.1).

At the lower rear of the cabinet is a removable plate, which provides alternative access for the cables.

2.2 Fitting the HSM into the Cabinet

2.2.1 Cam Locks

Two keys are required to fit an HSM into a cabinet and, subsequently, to open the HSM. One key is for the left-hand lock and the other for the right-hand lock (see Figure 1.1). The keys are unmarked when they leave the factory (except for a number tag). Note the tag numbers, because it is impossible to replace a key without this number (the keys CANNOT be copied legally by a locksmith). The keys are normally retained by independent security officers to provide dual control. Duplicate of each key are supplied with each unit.

For each HSM, make a note of its serial number and associated key tag numbers, and store this information in a secure location; it may be useful if a key needs to be replaced later.

To identify the correct key for each lock, use trial and error. Mark the keys for future identification (in accordance with the local/internal policy on secure physical keys) and remove the manufacturer's identification tag.

Similarly, mark the third key, used to operate the KEY switch on the rear of the unit (see Figure 1.9). A duplicate is also supplied with each unit.

2.2.2 Fitting the HSMs to the Sliding Runners

Each HSM is mounted in the cabinet on sliding runners. Install the lowest unit first in the cabinet (to avoid tipping). Install an HSM as follows:

- Slide the applicable pair of runners out from the cabinet to their full extent (until they lock into position).
- Offer the fixed tracks attached to the HSM to the runners extended from the cabinet, and slide the HSM backwards into the cabinet by 50 to 80 mm (2 to 3in) until it can go no further.
- On each track there is a spring-loaded button. Press the buttons inwards simultaneously and push the HSM backwards a few inches until it can go no further. The buttons have now locked into holes half way along each runner.
- Press the buttons simultaneously and push the HSM backwards.
- The HSM cannot be located fully in the cabinet without the keys to the cam locks. Use the keys to rotate each lock one quarter of a turn clockwise and push the HSM completely into the cabinet.
- Rotate the keys one quarter of a turn anti-clockwise to lock the HSM in position.

2.3 Opening and Closing the HSM

WARNING: SEE THE WARNINGS IN APPENDIX F.

To gain access to inside the HSM:

- Unlock the cam locks.
- Lower the front panel on its hinges.
- Slide the unit out of the cabinet.
- Remove the top from the unit by sliding it forwards then lift it off.

To close the HSM:

- Refit the top cover.
- Slide the unit back into the cabinet.
- Close the front panel.
- Lock the two cam locks and remove the two keys.
- If necessary, remove the key from the KEY switch on the rear panel.
- Press the RESET button on the rear panel.

2.4 Power Supply and Fuses

Ensure the connection of power to the units does not create a circuit overload conditions within the supply circuit and wiring. Ensure a reliable earth is maintained to all units.

2.4.1 Changing the Mains Fuse

WARNING: ALWAYS REMOVE THE POWER CABLE FROM THE HSM POWER INPUT CONNECTOR BEFORE ATTEMPTING TO CHANGE ANY FUSE.

The mains fuse holder is located in the power module at the rear of the unit. To gain access to the fuse (1.6 A, 20 mm type), use a screwdriver blade to spring-off the cover on the power module.

2.5 Preparing the HSM for Use

2.5.1 Connecting Power

A power cable suitable for the local mains connectors is supplied with each HSM. Plug the cable into the IEC style connector on the power module at the rear of the HSM. There is no on/off switch on the HSM, and when it is connected and power is turned-on, the HSM is ready to operate.

2.5.2 Cold Start

Always carry-out the Cold Start procedure before proceeding with the installation of the HSM. Refer to Cold Start, Chapter 3.

2.5.3 Connecting the Battery

The battery, which is a non-rechargeable Lithium Bromine complex cell, maintains the Local Master Keys and software configuration parameters during power fail conditions. It is not normally connected when the equipment leaves the factory.

To install the battery jumper, open the HSM.

Ensure that power is connected before installing the battery jumper JPR6 which is located near the right-hand edge of the Processor circuit board (see Figure 3.1 and Figure 3.2).

3 CONNECTING TO THE CONSOLE TERMINAL

The HSM has three RS-232-C connectors on the rear (see Figure 1.9). The right-hand connector (viewed from the rear of the unit) is for connection to an asynchronous ASCII Console terminal. The connector is an industry standard D-type 25-way female connector (socket) with screw fittings.

The Console is required during installation, and for operations in which secret data is entered into the HSM.

The Console is not supplied with the equipment and must be provided by the user. It is connected to the HSM by a cable, also user-supplied, which must not be more than 50ft (1524cm) in length.

3.1 Console Specification

Character set	:	ASCII
Interface	:	RS-232-C (DTE)
Baud	:	300 bps (and up to 38,400 bps)
Stop bits	:	1
Data bits	:	7 or 8
Parity	:	Odd, even or none
Flow control	:	XON, XOFF

The Console must not be able to store information and display it at a later time (because some data may be of a sensitive nature).

Character transmission rates and formats are specified by the user and can be configured at the time of HSM installation. The Console must be capable of operating at one of the HSM factory default settings. See Chapter 3.

RTS must be asserted to allow output from the HSM.

3.2 Console and Auxiliary Port Interface Signals

Pin	Signal	Details
1	Protect Ground	Can be connected to the HSM chassis by JPR12
2	TX Data	To HSM
3	RX Data	From HSM
4	RTS (Request To Send)	To HSM (Must be asserted)
5	CTS (Clear To Send)	From HSM (Always asserted)
6	DSR (Data Set Ready)	From HSM (Always asserted)
7	Signal Ground	
8	DCD (Data Carrier Detect)	From HSM (Always asserted)
15	TX Clock (DCE Source)	16 x Baud, from HSM
17	RX Clock (DCE Source)	16 x Baud, from HSM
20	DTR (Data Terminal Ready)	To HSM (Ignored)

3.3 Confirming Correct Console Configuration

Assuming the HSM default settings (as shipped from the factory, or after a cold start) apply, configure the Console as shown in Chapter 3, and for full duplex (no local echo).

Press the < Return > key. The HSM should respond with:

Online >

which indicates that correct communications have been achieved but a valid command has not been entered.

4 CONNECTING TO THE PRINTER

The printer is connected to the Auxiliary port, which is the left-hand D-type connector on the rear of the HSM (as viewed from the rear of the unit).

The baud and word format must be set using the Console CA command.

4.1 Printer Specification

Character set	:	ASCII
Interface	:	RS-232-C (DTE) serial data (not parallel)
Baud	:	300 to 38,400 bps
Stop bits	:	1
Data bits	:	7 or 8
Parity	:	Odd, even or none
Flow control	:	XON, XOFF

The paper feed mechanism should be sprocket-feed (not friction) to align print columns and lines.

The printer must be an impact printer (e.g. dot matrix or fully-formed characters). Thermal, laser, or similar printers are not suitable because mailer forms are multi-copy to keep PINs and key components secret.

The printer must be capable of operating without the ribbon to keep the information in the mailer secret.

The printer should be wide enough to accommodate the mailer forms that are in use.

5 CONNECTING TO THE HOST

5.1 Host Port Connections for Async, Bisync and SNA-SDLC/RS232

		ASCII Async	ASCII/EBCDIC Bisync and SNA-SDLC	
Pin	**Signal**	**DCE**	**DCE**	**DTE**
1	Protect Ground	Can be connected to the HSM chassis via jumper JRP 11		
2	TX Data	To HSM	To HSM	From HSM
3	RX Data	From HSM	From HSM	To HSM
4	RTS (Request To Send)	To HSM (Ignored)	To HSM (Ignored)	From HSM (Asserted if ready)
5	CTS (Clear To Send)	From HSM (Always asserted)	From HSM (Always asserted)	To HSM (Accepted)
6	DSR (Data Set Ready)	From HSM (Always asserted)	From HSM (Always asserted)	To HSM (Ignored)
7	Signal Ground			
8	DCD (Data Carrier Detect)	From HSM (Always asserted)	From HSM (Always asserted)	To HSM (Accepted)
15	TX Clock (DCE Source)	16 x Baud from HSM	At Baud from HSM	At Baud to HSM
17	RX Clock (DCE Source)	16 x Baud from HSM	At Baud from HSM	At Baud to HSM
20	DTR (Data Terminal Ready)	To HSM (Ignored)	From HSM (Always asserted)	From HSM (Always asserted)
23	Data Rate Select	Not connected	Not connected	Not connected
24	TX Clock	To HSM (Ignored)	To HSM (Ignored)	

5.2 Host Port Connections for SDLC/RS-449

The table shows the SDLC/RS-449 port pin connections for the 37-way female D Type connector.

Pin	Signal	Details
1	Protect Ground	Can be connected to the HSM chassis via jumper JPR 1 on the SDL Interface board.
2 and 3	Not connected	
4	SD-Input	Send Data
5	ST - Output (At Baud)	Send Timing
6	RD - Output	Received Data
7	RS - Input (Monitored)	Request To Send
8	RT - Output (At Baud)	Receive Timing
9	CS - Input (Connected To RS)	Clear To Send
10	Not connected	
11	DM - Output (Asserted)	Data Mode
12	TR - Input (Ignored)	Terminal Ready
13	RR - Output (Asserted During Tx)	Receiver Ready
14 to 17	Not connected	
18	TM Output (Negated)	Test Mode
19	SG	Signal Ground
20	RC	Receive Common
22	SD + Input	Send Data
23	ST + Output (At Baud)	Send Timing
24	RD + Output	Receive Data
25	RS + Input (Monitored)	Request To Send
26	RT + Output (At Baud)	Receive Timing
27	CS + Input (Connected To RS)	Clear To Send
28	Not connected	
29	DM + Output (Asserted)	Data Mode
30	TR + Input (Ignored)	Terminal Ready
31	RR + Output (Asserted During Tx)	Receiver Ready
32 to 37	Not connected	

5.3 Host Port Connections for SNA-SDLC/V.35

The table shows the V.35 port pin connections for the 34-way female connector (J2 on the V.35 Interface board). Not all pin positions are used, and only those pins that are used are fitted to the connector housing.

Pin	Signal	Details	
A	Protective Ground	Can be connected to the HSM chassis via JPR5/1 on the V.35 Interface board.	
B	Signal Ground	Can be connected to the HSM Chassis via JPR5/2.	
		DCE	DTE
C	RTS (Request To Send)	Input (ignored)	Output (asserted if HSM has data to send)
D	CTS (Clear To Send)	Output (always asserted)	Input (required for HSM to send data)
E	DSR (Data Set Ready)	Output (always asserted)	Input (ignored)
F	RLSD (equivalent to DCD) (Rx Line Signal Detect)	Output (always asserted)	Input (ignored)
P	TxD (A) (Transmit Data)	Input	Output
S	TxD (B)		
R	RxD (A) (Receive Data)	Output	Input
T	RxD (B)		
Y	TxCk (A) (Transmit Clock)	Output (at Baud)	Input (at Baud)
AA	TxCk (B)		
V	RxCk (A) (Receive Clock)	Output (at Baud)	Input (at Baud)
X	RxCk (B)		
U	DTE TxCk (A) (Tx Clock)	Input (at Baud) (not used)	Output (at Baud)
W	DTE TxCk (B)		

CHAPTER 3

CONFIGURATION

CONTENTS

Page

1 GENERAL 3-1

2 INTERNAL OPTIONS 3-1
2.1 INTERNAL OPTION JUMPERS 3-1
2.1.1 COLD START 3-1
2.1.2 MOVEMENT DETECTOR 3-1
2.1.3 DES CHIP SELECTOR JUMPERS 3-1
2.2 INTERNAL OPTION SWITCHES 3-2
2.2.1 CONSOLE PORT DEFAULT SETTINGS 3-2
2.2.2 DSP MODULE 3-2
2.2.3 BUFFER SIZE SELECTION 3-2

3 CONFIGURING THE CONSOLE PORT 3-5

4 CONFIGURE SECURITY / QUERY SECURITY COMMANDS 3-6

5 CONFIGURING THE AUXILIARY PORT 3-9
5.1 DEFAULT SETTINGS (AUXILIARY PORT) 3-9

6 CONFIGURING THE HOST PORT 3-10
6.1 ASYNCHRONOUS EMULATION 3-10
6.1.1 SETTING THE JUMPERS FOR DCE OPERATION 3-10
6.1.2 MESSAGE HEADER LENGTH 3-10
6.1.3 TRANSPARENT ASYNCHRONOUS COMMUNICATIONS 3-11
6.1.4 CONFIGURING THE SOFTWARE 3-11
6.2 BISYNCHRONOUS EMULATION 3-14
6.2.1 MESSAGE HEADER LENGTH 3-14
6.2.2 HOST ENVIRONMENT 3-14
6.2.3 DEFINING THE HOST PORT 3-15
6.2.4 BAUD AND WORD FORMATS 3-16
6.2.5 POLL/SELECT ADDRESS 3-16
6.2.6 CONFIGURING THE SOFTWARE 3-16
6.3 IBM CHANNEL INTERFACE (FIPS 60) 3-20
6.3.1 CONNECTING POWER 3-20
6.3.2 SETTING THE SUB-CHANNEL ADDRESS 3-20
6.3.3 CONNECTING TO THE IBM CHANNEL 3-21
6.3.4 CHANNEL INTERFACE 3-26
6.4 SDLC EMULATION 3-28
6.4.1 MESSAGE HEADER LENGTH 3-28
6.4.2 STATION ADDRESS 3-28
6.4.3 SETTING THE JUMPERS FOR DCE OPERATION 3-28
6.4.4 CONFIGURING THE SOFTWARE 3-30
6.5 SNA-SDLC SYNCHRONOUS EMULATION 3-32
6.5.1 COMMAND MESSAGE FORMAT 3-32
6.5.2 MESSAGE HEADER LENGTH 3-32

6.5.3 TRANSPARENT DATA MODE 3-32
6.5.4 CHARACTER SET 3-33
6.5.5 HOST ENVIRONMENT 3-33
6.5.6 SDLC STATION ADDRESS 3-33
6.5.7 BAUD RATE AND WORD FORMAT 3-33
6.5.8 DEFINING THE RS-232-C HOST PORT 3-34
6.5.9 DEFINING THE V.35 HOST PORT 3-35
6.5.10 CONFIGURING THE SOFTWARE 3-37
6.6 ETHERNET 3-39
6.6.1 CONFIGURING THE HARDWARE 3-39
6.6.2 CONFIGURING THE SOFTWARE 3-39

7 PROGRAMMING GUIDE 3-42
7.1 ASYNCHRONOUS CONNECTED OPTION 3-42
7.2 TRANSPARENT ASYNCHRONOUS CONNECTED OPTION 3-42
7.2.1 SENDING COMMANDS 3-42
7.2.2 HSM PROCESSING OF PACKETS 3-42
7.2.3 PARITY ERRORS 3-43
7.3 BISYNCHRONOUS CONNECTED OPTION 3-43
7.4 CHANNEL ATTACH OPTION 3-43
7.4.1 IOGEN CONSIDERATIONS 3-44
7.4.2 HSM CHANNEL COMMANDS AND OPERATION 3-44
7.4.3 UNIT STATUS AND SENSE INFORMATION 3-45
7.4.4 SAMPLE TEST PROGRAM 3-46
7.5 SNA-SDLC CONNECTED OPTION 3-46
7.5.1 SESSION COMPONENTS 3-46
7.5.2 SUPPORTED COMMANDS 3-47
7.5.3 DIFFERENCES AND EXCEPTIONS 3-47
7.5.4 HOST SNA SESSION CONSIDERATIONS 3-47
7.5.5 HOST NCP CONFIGURATION 3-51
7.6 TCP/IP PROTOCOL 3-51
7.6.1 SENDING COMMANDS 3-51
7.6.2 RETURNING RESPONSES 3-52
7.7 UDP PROTOCOL 3-52
7.7.1 SENDING COMMANDS 3-53
7.7.2 RETURNING RESPONSES 3-53

1 GENERAL

This chapter describes how to physically configure the HSM to fit into the Host system.

2 INTERNAL OPTIONS

2.1 Internal option Jumpers

Some options are configured by the use of small jumpers (electrical connectors). A jumper is fitted by pushing it over a pair of small pins which are mounted vertically on the printed circuit board.

2.1.1 Cold Start

All software-configurable parameters have factory-set default conditions. When the battery has been connected, any changes made via the Console are stored in battery-protected memory. If it becomes necessary to re-select the factory conditions, this can be achieved by using the "Cold Start" jumper (this is normally needed only if the setting for the baud or the word format selected for the Console is forgotten, or if new firmware PROMs have been fitted).

The procedure is:

1. Remove the Battery jumper from the pins of JPR6.
2. Place the jumper on the pins of JPR4 (Cold Start).
3. Remove the HSM's power lead, then re-connect it after a delay of 20 seconds.
4. Remove the Cold Start jumper from the pins of JPR4.
5. Re-place the jumper on the pins of JPR6 (Battery).

When the cold start is used, all software-selectable options are returned to their default settings. Therefore, if the system is operational and it does not use the default settings, the various options must be returned to their required settings.

2.1.2 Movement Detector

The movement detector within the HSM is enabled by removing JPR 16. It is activated when the HSM is armed.

2.1.3 DES Chip Selector Jumpers

The HSM supports two types of DES chip 2001 and 20C03 and also supports two modes of operation for the 20C03 type. JPR 3 as seen in figure 3.1 selects the DES Chip type and mode of operation. The mode of operation is specific to the firmware if the wrong mode is selected DES Chip Error will be generated at reset. Base release firmwares 5.04 or later require the DES chip to operate in the 20C03HS mode.

2.2 Internal Option Switches

SW2 supplies certain options these are defined as follows,

SW2 - 1 - Enable SDLC within standard firmware
SW2 - 2 - Select default Console Port settings
SW2 - 3 - Enable DSP Module
SW2 - 4 - Buffer size selector (Only used on HS variants)
SW2 - 5, 8 - reserved for future use.

2.2.1 Console Port Default Settings

The default settings for the Console port, to which the unit defaults after a cold start, can be set by SW2-2 (Figure 3.1 and **Figure 3.2**) to be either:

SW2-2 OFF (open)	SW2-2 ON (closed)
300 bps	19200 bps
7 data bits	8 data bits
1 stop bit	1 stop bit
Odd parity	No parity

2.2.2 DSP module

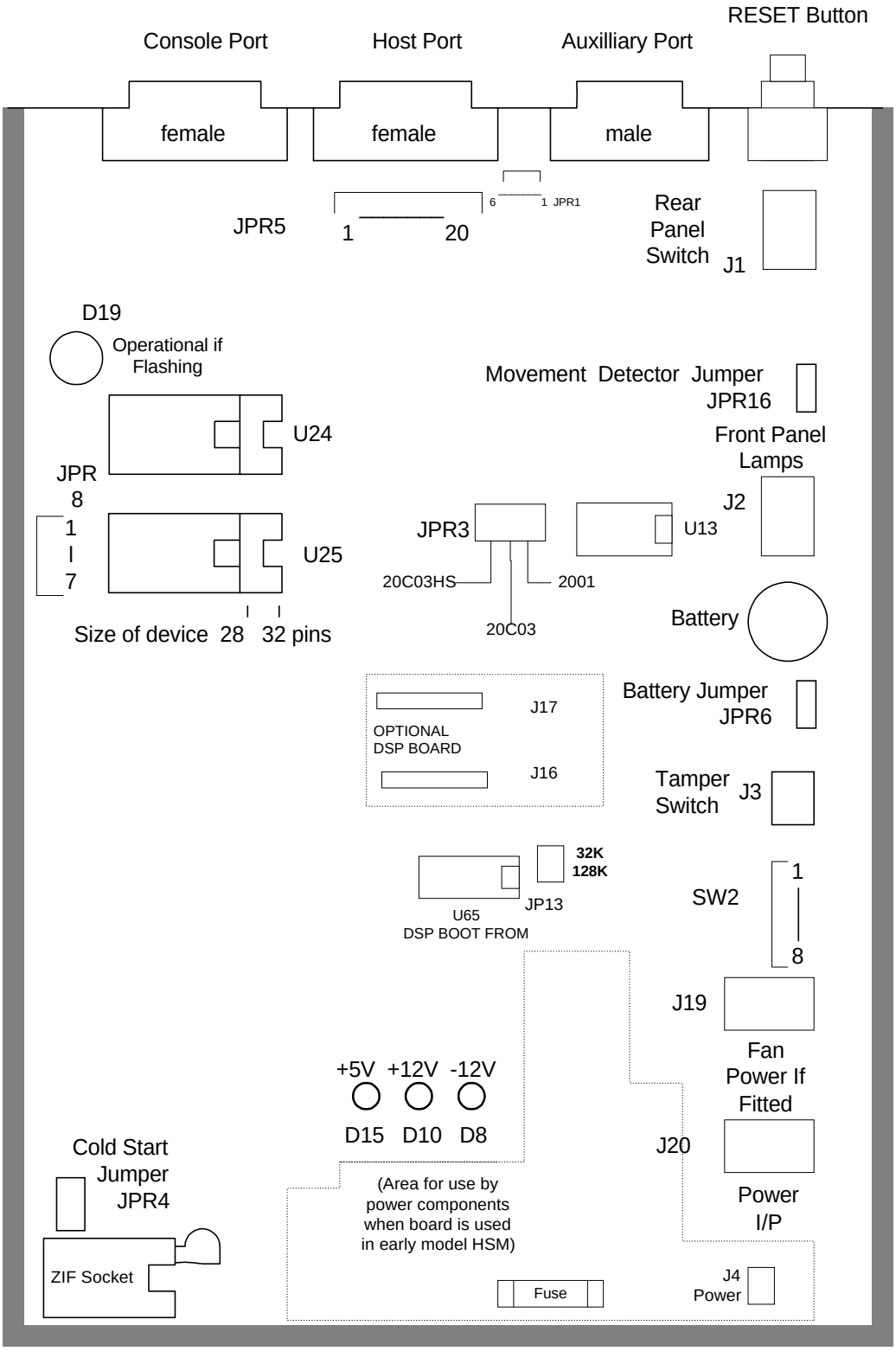
If an optional DSP module and associated DSP Boot prom is fitted SW 2-3 must be in the ON (closed) position.

2.2.3 Buffer Size Selection

This switch indicates the size of the I/O buffer enabled within an RG7210 this will be set at production time.

SW2 - 4 OFF (open) - 8k buffer
SW2 - 4 ON (closed) - 16k buffer

Figure 3.1 - Processor Circuit Board, 20153D1 Rev 2.0



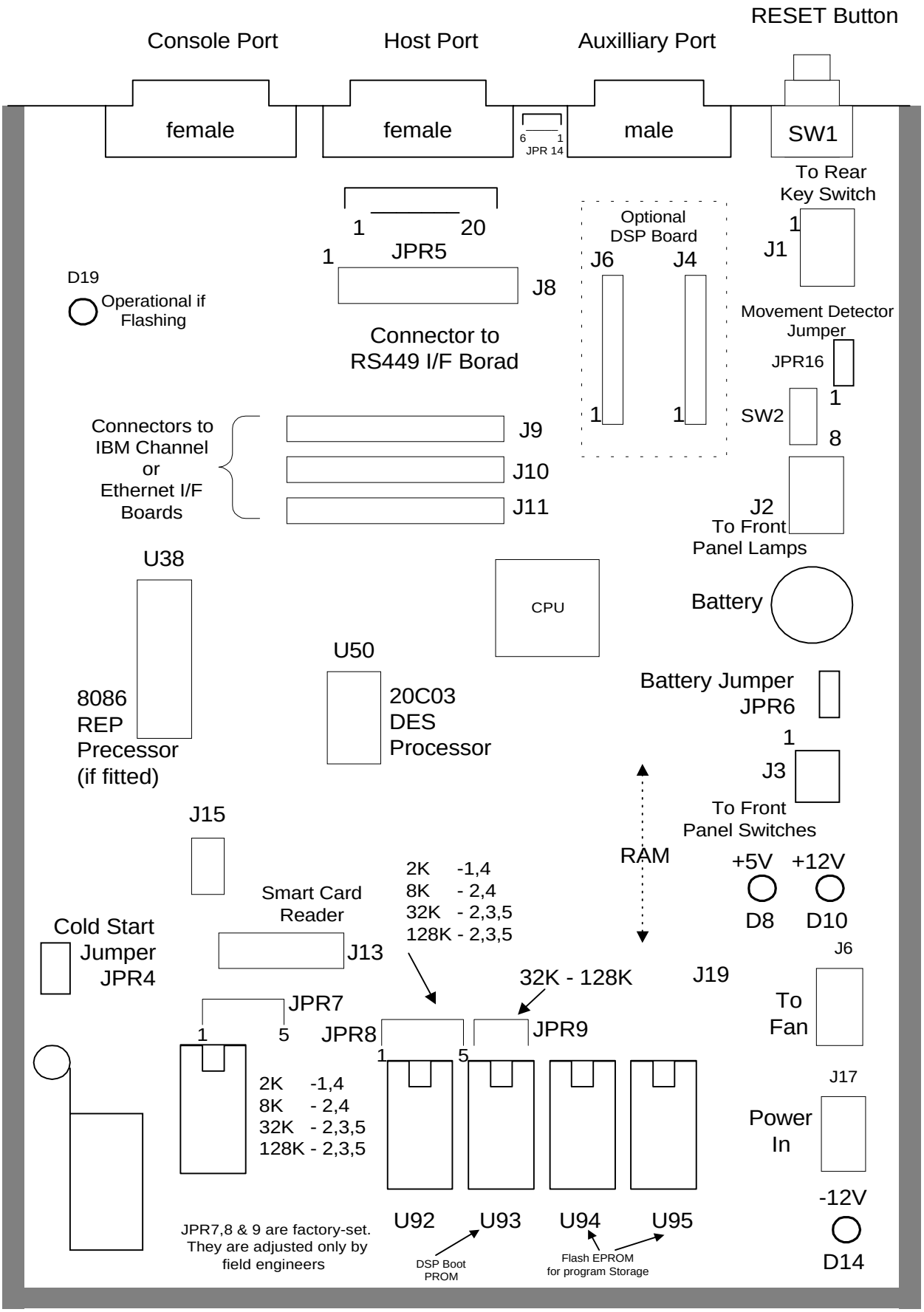


Figure 3.2 - High Speed HSM Circuit Board

3 CONFIGURING THE CONSOLE PORT

The HSM Console port can be configured while the HSM is in either the online or the offline state.

Enter CC < Return > (Configure Console) to initiate the following example in which user input is shown underlined. The Console baud is to be changed to 9600, and the word format is to be changed to 8 data bits, no parity and one stop bit.

Example:

Offline > CC < Return >

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or <RETURN> for no change.

Console baud rate: (current value = 1) 6 <Return>
Console word format: (current value = 2) 4 <Return>

Offline>

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

4 CONFIGURE SECURITY / QUERY SECURITY COMMANDS

The security configuration of the HSM and some processing parameters are set by the CS (Configure Security) Console command; the settings can be examined by the QS (Query Security) Console command. The HSM must be offline.

The parameters concerned are:
PIN length, Default: 4.
Echo Password and Secret Values to Console. Default: off.
ZMK variant support for interoperation with Atalla systems. Default: off.
Racal or Australian transaction key support. Default: Racal
User storage key length. Default: Single
Availability of clear PIN facilities. Default: no.
Availability of ZMK translate command. Default: No.
Availability of ANSII X9.17 methods for importing keys. Default: No.
Availability of ANSII X9.17 methods for exporting Keys. Default : No
PIN solicitation batch size. Default: 1536.
Zone Master Key length. Default: single.
Choice of PIN encryption algorithm. Default: A (Compatible with RG6000 range HSMs).
Smart Card or Password control of the Authorized state. Default: Card.
Smart Card “Manufacturer’s issuer password”. Default: GUARDATA.

The QS command reports the states of the parameters, plus the LMK check value.

The default conditions are set after a ‘Cold Start’. (Paragraph 2.2)

The HSM stores encrypted PINs as one character greater than the length of the PIN; it must therefore be informed of the maximum length of PINs.

It can be set to allow clear PINs to be returned to the Host so that the Host (instead of the HSM) can print PIN mailers.

THE HSM CLEAR PIN FACILITY PRESENTS A SECURITY RISK UNLESS ADEQUATE PRECAUTIONS ARE TAKEN AT THE HOST.

The HSM can process PIN solicitation data in batch mode. As a security measure, it does not process the data until it reaches a minimum batch size.

The CS command prompts for PIN length, Echo on/off, Atalla variant support and Racal or Australian transaction key support which do not require the LMKs to be cleared. It also prompts for clearing (zeroizing) the LMKs, which is necessary if any of the other parameters are to be changed.

The Translate ZMK function is disabled on running the CS command. It can be re-enabled after clearing the LMKs.

CS Inputs: PIN Length: a one or two-digit number, (4 to 12).
Echo: N or F (oN or ofF).
Atalla ZMK variant support: N or F (oN or ofF).
Racal or Australian transaction key: [R/A]:
User storage key length (Single/Double/Triple):
Erase LMKs, confirm Y or N.
Select clear PINs: Y or N
Enable ZMK translate command: Y or N
Enable X9.17 for import: Y or N
Enable X9.17 for export: Y or N
Solicitation batch size: a one to four-digit number, 1 to 1535.
Single/double ZMKs: S or D (Single or Double).
PIN encryption algorithm: A or B (Visa method or Racal Method)
Card / password authorisation: C or P (Card or Password).
Card issuer password: 8 alphanumeric printable characters. (ENTER = nochange)

CS Outputs: Prompts as shown below.

CS Errors: If entered value is out of range, the HSM re-prompts for an input.

QS Outputs: PIN Length:
Encrypted PIN length:
Echo:
Atalla ZMK variant support:
Transaction key support:
User storage key length:
Select clear PINs:
Enable ZMK translate command:
Enable X9.17 for import:
Enable X9.17 for export:
Solicitation batch size:
ZMK length: S or D.
PIN encryption algorithm:
Card/password authorisation:
LMK check:
Old LMK loaded:

CS and QS convert all lower-case alpha values to upper case for display purposes, except for the Card issuer Password. Operation is menu-driven, as shown in the examples.

Examples:

Offline> CS < Return >
PIN Length [4-12]: 4 < Return >
Echo [oN/ofF]: N < Return >
Atalla ZMK variant support [oN/ofF]: F
Racal or Australian transaction key [R/A]: R
User storage key length [Single/Double/Triple]: S

LMKs must be erased before remaining parameters can be set.
Erase LMKs? [Y/N]: N < Return >

Offline> CS < Return >
PIN Length [4-12]: 4 < Return >
Echo [oN/ofF]: F < Return >
Atalla ZMK variant support [oN/ofF]: F
Racal or Australian transaction key [R/A]: R
User storage key length [Single/Double/Triple]: S

LMKs must be erased before remaining parameters can be set.
Erase LMKs? [Y/N]: Y < Return >

Select clear PINs? [Y/N]: N < Return >
Enable ZMK translate command [Y/N]: N < Return >
Enable X9.17 for import [Y/N]: N < Return >
Enable X9.17 for export [Y/N]: N < Return >
Solicitation batch size [1-1535]: 1024 < Return >
Single/double length ZMKs [S/D]: S < Return >
PIN encryption algorithm [A/B]: A < Return >
Card/Password authorisation [C/P]: C < Return >
Card issuer password [Enter = no change]: < Return >

Online > QS < Return >
PIN length: 4
Encrypted PIN length: 5
Echo: OFF
Atalla ZMK variant support: OFF
Racal or Australian transaction key: Racal
User storage key length: Single
Select clear PINs: No
Enable ZMK translate command: No
Enable X9.17 for import: No
Enable X9.17 for export: No
Solicitation batch size: 1024
ZMK length: S
PIN encryption algorithm: A
Card/password authorisation: C

Local Master Key Check = 0123 4567 89AB CDEF
Old LMK Loaded: No

The QS command displays the PIN length and the encrypted PIN length (the latter is referred to by some HSM Host commands).

5 CONFIGURING THE AUXILIARY PORT

The Auxiliary port can be configured while the HSM is in either the offline or the online state.

The variables to be configured are as follows:

- Baud rate : 300 to 38.4k.
- Data bits : 7 or 8 data bits.
- Parity bit: : Odd, even or no parity.
- Stop bit : 1 stop bit.

The procedure is similar to configuring the Console port. The following is an example of configuring the Auxiliary port for 9600 baud, 7 data bits, even parity and 1 stop bit.

Example: CA < Return >

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Auxiliary port baud rate: (current value = 6) <Return>
Auxiliary port word format: (current value = 4) 3 <Return>

The values entered take effect immediately after the command has been completed.

5.1 Default Settings (Auxiliary Port)

The default settings for the Auxiliary port, to which the unit defaults after a cold start, are:

9600 baud,
8 data bits,
1 stop bit,
No parity.

6 CONFIGURING THE HOST PORT

The HSM Host interface can be configured via the Console to emulate a number of types of data communications equipment and control equipment. (A list is shown in the table in Chapter 1).

6.1 Asynchronous Emulation

In Asynchronous Emulation the HSM is viewed by the Host as a DCE (data communications equipment) device, and does not require a modem. The electrical interface between the Host and the HSM conforms to the RS-232-C standard. This is the configuration in which the HSM is shipped from the factory.

To configure the HSM for asynchronous communications:

- The port must be defined as a DCE.
- Details held in software must be configured.

The following variables can be configured:

- The required length of the message header. This is normally set to 4, but can be set between 1 and 255. This depends on the value used by the Host computer application.
- The baud rate of the Host computer port.
- The word format of the Host computer port.
- The required communications protocol, either standard or transparent asynchronous ASCII.
- The asynchronous terminating characters. The terminating sequence can be either one or two characters. To select the terminating characters four hexadecimal values must be entered. If only one terminating character is required, enter the first two hexadecimal values followed by 00.

6.1.1 Setting the Jumpers for DCE Operation

For DCE operation, the applicable jumpers are inserted on a row of pins, JPR5 (see Figure 3.1 and Figure 3.2).

Power must be disconnected before any jumpers are fitted or removed. For access, see Figure 3.3 shows the jumper positions for DCE configuration.

6.1.2 Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

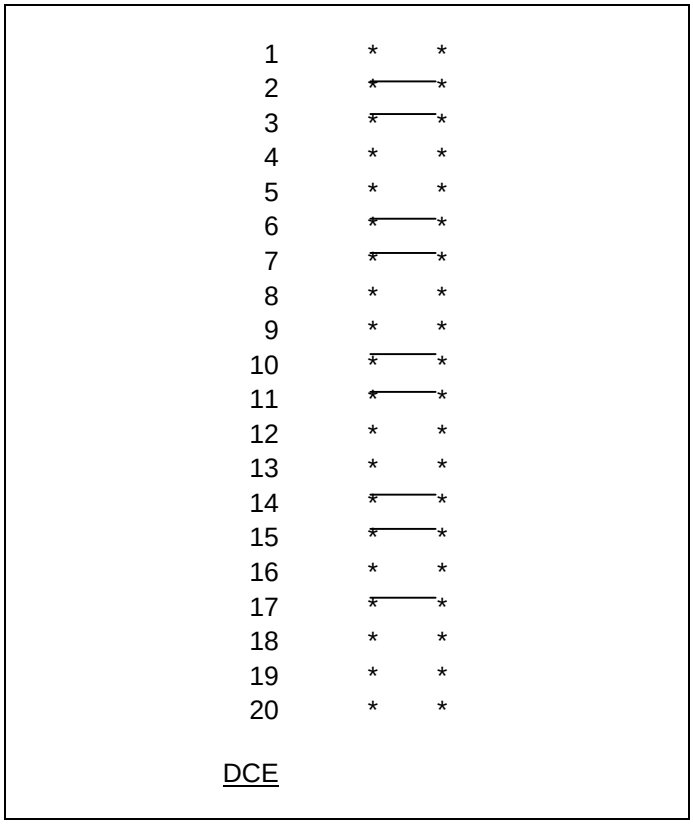


Figure 3.3 - The Jumpers on JPR5 for DCE Operation

6.1.3 Transparent Asynchronous Communications

In the standard asynchronous mode of communication, codes like STX (X'02) and ETX (X'03) have a special meaning, but they can sometimes occur in a stream of binary data, where that special meaning does not apply.

To avoid ambiguity, Transparent Asynchronous Communications mode is used. This has a simplified message format (for details see the Programmers Manual).

The Host port of the HSM must be configured for Transparent Async Communications and 8-bit data transfers.

6.1.4 Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key in the KEY switch on the rear panel and rotate it clockwise a quarter turn, then allow it to spring back), with power applied and the Console terminal connected.

The Console displays:

HSM going OFFLINE, press Reset to go Online.
Master Key loading facilities now available.

Offline>
Enter CH < Return > (Configure Host) to initiate the set-up dialogue. Examples of the standard and transparent asynchronous configurations are described as follows. User inputs are shown underlined.

6.1.4.1 Standard Asynchronous Communications

In the example, standard asynchronous communications is enabled, the message header length is 4 characters and the terminating characters are set to 0300 hexadecimal (ETX). The Host baud is changed from 300 to 19200 bps; the word format to 8 data bits, no parity and 1 stop bit.

Example:

Offline> CH < Return >

Message header length (1-255): 4
Asynchronous/Bisynchronous 3270 (A/B): A
Transparent mode (Y/N): N
Terminating characters (4 hex): 0300

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 1) 7< Return >
Host word format: (current value = 2) 4< Return >

Offline>

After completing the procedure reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.1.4.2 Transparent Asynchronous Communications

In the example, transparent asynchronous communications is enabled and the message header length is set to 6 characters.

The Host baud is changed to 9600 bps and the word format is set to 8 data bits, no parity and 1 stop bit. No option of message terminating characters is offered because this is fixed (value X'03, "ETX" character).

Example:

Offline> CH < Return >

Message header length (1-255): 6
Asynchronous/Bisynchronous 3270 (A/B): A
Transparent mode (Y/N): Y

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 1) 6 < Return >
Host word format: (current value = 2) 4 < Return >

Offline>

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.2 Bisynchronous Emulation

The HSM supports the IBM 3270 Bisynchronous Communications protocol. It has a number of user-configurable bisynchronous communications options. The electrical interface between the Host and the HSM conforms to the RS-232-C standard. The following variables can be configured:

- The message header length (1 to 255 characters).
- The character set can be either EBCDIC or ASCII.
- The HSM can support the IBM IMS and CICS host environments.
- The Host interface can be either a DCE or a DTE.
- The baud rate and word format can be selected (if DCE).
- The 3274 poll/select address

6.2.1 Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

6.2.2 Host Environment

The HSM can be made compatible with an IBM Host running applications under IMS or CICS.

6.2.2.1 IMS

In IMS applications, the HSM requires the entry of one or more test strings to enable it to distinguish between valid transactions and system error and status messages. When the Host software is written, the programmer must insert one of the test strings in the message header field of each valid transaction to the HSM.

The HSM searches for the strings and accepts a transaction only if it contains one of them. It allows a maximum of 20 characters (including delimiters) to be entered. The strings, delimited by commas, can contain any alphanumeric character, and do not need to be the same length. If more than one string is defined, the HSM accepts a transaction if it matches any one of them.

In addition, a test string offset is required. This value allows the test string to be placed at any fixed position in the message header, by specifying the number of characters to skip before the comparison is made. It can be any value from zero to the message header length (but if the header length minus the offset is less than the length of a test string, that particular string will never be found).

All messages that do not have one of the test strings at the defined offset are ignored, and the HSM responds with a PA2 AID at the next poll.

6.2.2.2 CICS

In CICS applications, the HSM searches the beginning of each transaction for the DFH string, which identifies all CICS system messages. If it is found, the message is ignored and the HSM responds with the CLEAR AID at the next poll.

6.2.3 Defining the Host Port

For Synchronous operation, the HSM can be set for either DCE or DTE operation. The applicable jumpers are inserted on a row of pins, JPR5, on the Processor circuit board (see Figure 3.1 and Figure 3.2 /Figure 3.4).

Disconnect power before fitting or removing the jumpers. For access, see Chapter 2.

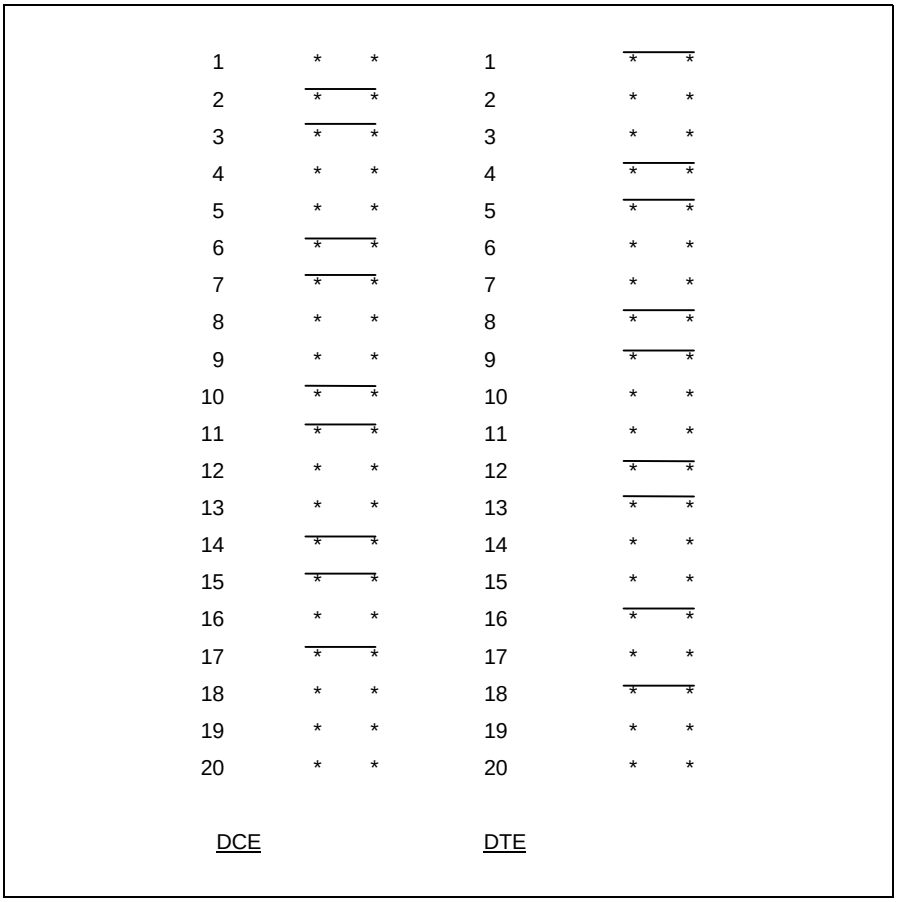


Figure 3.4– The Jumpers onJPR5 for DCE or DTE Operation

The selected option must also be defined during the software configuration process.

Note that when DCE operation is selected, the HSM provides the synchronous clock signals.

NOTE: WHEN DTE OPERATION IS SELECTED, THE HOST SYSTEM MUST PROVIDE THE CLOCK SIGNALS.

6.2.4 Baud and Word Formats

The baud for the Host port can be set to 300, 600, 1200, 2400, 4800, 9600, 19200, or 38400 bps.

For a bisynchronous Host port, the word format is automatically chosen with the character set:

- Seven data bits and odd parity for ASCII.
- Eight data bits and no parity for EBCDIC.

6.2.5 Poll/Select Address

The address used to poll/select the HSM is a 4 hexadecimal character value. This address must comply with the CU device number selected in the NCP. The poll/select address is set with the CH command.

In Bisynchronous operation the HSM emulates a 3720 Control Unit (CCU) with one terminal device attached. It responds to both General and Specific polls, in addition to Selects. If the Poll/Select address 4060 is chosen, the HSM responds to the following address combinations:

General Poll	40407F7F
Specific Poll	40404040
Select	60604040

These default address combinations correspond to CU0, device 0.

6.2.6 Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key into the KEY switch on the rear panel, and rotate it clockwise a quarter turn, then allow it to spring back), with power applied and the Console connected.

The Console displays:

HSM going OFFLINE, press Reset to go Online.

Master Key loading facilities now available.

Offline>

Enter CH < Return > (Configure Host) to initiate the set-up dialogue. Examples of the various bisynchronous configurations are described below. User inputs are shown underlined.

6.2.6.1 EBCDIC Character Set, No IMS or CICS, DCE

In the example, the EBCDIC character code is selected, the Host port is DCE, the message header is 4 characters and the poll/select address is set to X'C5E5. The Host baud is changed to 19200 bps, and no selection is offered for the word format.

Example: CH < Return >

Message header length (1-255): 4
Asynchronous/Bisynchronous 3270 (A/B): B
EBCDIC/ASCII (E/A): E
Poll/select address (4 hex): C5E5
IMS/CICS/General (I/C/G): G
DTE/DCE (T/C): C

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 6) 7 < Return>

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.2.6.2 ASCII Character Set, No IMS or CICS, DTE

In the example, the ASCII character code is selected, the Host port is DTE, the message header is 10 characters and the poll/select address is set to X'4060. No Host baud is offered because the port is configured as a DTE.

Example: CH < Return >

Message header length (1-255): 10
Asynchronous/Bisynchronous 3270 (A/B): B
EBCDIC/ASCII (E/A): A
Poll/select address (4 hex): 4060
IMS/CICS/General (I/C/G): G
DTE/DCE (T/C): T

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.2.6.3 EBCDIC Character Set, CICS Support, DCE

In the example, CICS support is selected, the EBCDIC character code is selected, the host port is DCE, the message header is 4 characters and the poll/select address is set to X'4F6F. No change is made to the host baud, and no selection is offered for the word format.

Example: CH < Return >

Message header length (1-255): 4
Asynchronous/Bisynchronous 3270 (A/B): B
EBCDIC/ASCII (E/A): E
Poll/select address (4 hex): 4F6F
IMS/CICS/General (I/C/G): C
DTE/DCE (T/C): C

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 6) < Return >

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.2.6.4 EBCDIC Character Set, IMS support, DCE

In the example, IMS is selected, the EBCDIC character code is selected, the Host port is DCE, the message header is 20 characters, and the poll/select address is set to X'4F6F. The host baud is changed to 19200 bps, and no selection is offered for the word format.

Example: CH < Return >

Message header length (1-255): 20
Asynchronous/Bisynchronous 3270 (A/B): B
EBCDIC/ASCII (E/A): E
Poll/select address (4 hex): 4F6F
IMS/CICS/General (I/C/G): I
IMS message identifier (1-20): PIN,MAC
Identifier offset: 3
DTE/DCE (T/C): C

BAUD RATES		WORD FORMATS	
1.	300	1.	7 bits, no parity, 1 stop
2.	600	2.	7 bits, odd parity, 1 stop
3.	1200	3.	7 bits, even parity, 1 stop
4.	2400	4.	8 bits, no parity, 1 stop
5.	4800	5.	8 bits, odd parity, 1 stop
6.	9600	6.	8 bits, even parity, 1 stop
7.	19200		
8.	38400		

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 6) 7 < Return >

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.3 IBM Channel Interface (FIPS 60)

6.3.1 Connecting Power

Mains power is supplied to the HSM via the power input module. Each HSM is independent and requires its own power input (115/230 Volts). If the Host computer runs from an uninterruptable power supply (UPS), the HSM should be connected to the same supply. Otherwise, run the HSM units on different phases, if possible, so that if one phase fails, the remaining units continue to operate.

At power-on and after a reset, the HSM performs self-tests. When the Processor circuit board has completed its test, it checks whether the Channel Interface board has completed its tests successfully by sending an Attention signal. If the Channel Interface board is operating correctly, it responds to the Attention signal. The Processor circuit board waits up to one minute for the Channel Interface board to respond, and if there is no response within this time, the processor circuit board sends the following message to the Console port:

CHANNEL I/O ERROR: NO RESPONSE TO ATTN

This indicates a hardware problem which should be investigated.

To view this message, connect a terminal to the Console port of the HSM, configured to one of the HSM default settings. For an HSM that has already been installed and is being powered up again, the setting should match those programmed in the HSM.

Whenever the HSM is powered up or reset, a terminal should be connected to the Console port to determine whether an error message is displayed.

6.3.2 Setting the Sub-Channel Address

The HSM uses a single sub-channel address which must be even (i.e., 0, 2, 4, ... X'FC, X'FE). The location of the address switches SW1 on the Channel Interface board are shown
Figure 3.5 The settings are shown in the table that follows. Note that switch 1 must always be ON.

Figure 3.5 also shows switches SW2, which must always be OFF.

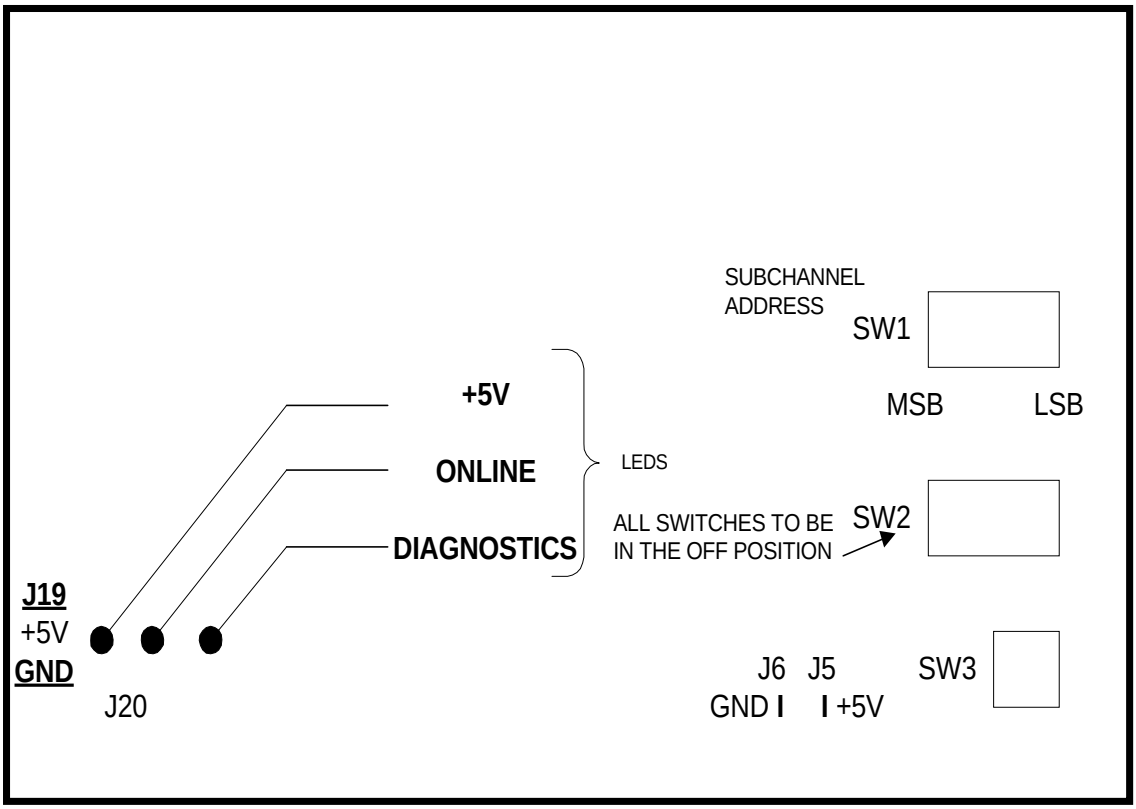


Figure 3.5 - Channel Interface Circuit Board

6.3.3 Connecting to the IBM Channel

Before connecting the HSM to the channel, verify that there is no I/O activity on the channel. The TAG OUT and BUS OUT cables are for connection to control units or HSMs that are further downline from the HSM. Note that "opposite connector colours mate" (i.e., a dark channel cable connector mates to a light cable connector and vice versa). If the HSM is the last downline control unit, insert standard terminator blocks into the TAG OUT and BUS OUT connectors.

6.3.3.1 Control Unit Selection

The channel attach option emulates a basic tape control unit with limited command capabilities and can be connected to any computer byte or block multiplexer channel meeting the IBM specification GA22-6974. It can also interface with any plug-compatible equivalent channel that conforms to the NBS FIPS-60 specification. Manufacturers include Amdahl, Fujitsu, HDS, Unisys, etc. The IBM range includes 360, 370, 4300 series, 3080 series, 3090 series and ES9000 series

	SUB-CHANNEL ADDRESS SELECT SWITCH SW1							
ADDRESS	8	7	6	5	4	3	2	1
00	ON	ON	ON	ON	ON	ON	ON	ON
02	ON	ON	ON	ON	ON	ON	OFF	ON
04	ON	ON	ON	ON	ON	OFF	ON	ON
06	ON	ON	ON	ON	ON	OFF	OFF	ON
08	ON	ON	ON	ON	OFF	ON	ON	ON
0A	ON	ON	ON	ON	OFF	ON	OFF	ON
0C	ON	ON	ON	ON	OFF	OFF	ON	ON
0E	ON	ON	ON	ON	OFF	OFF	OFF	ON
10	ON	ON	ON	OFF	ON	ON	ON	ON
12	ON	ON	ON	OFF	ON	ON	OFF	ON
14	ON	ON	ON	OFF	ON	ON	OFF	ON
16	ON	ON	ON	OFF	ON	OFF	OFF	ON
18	ON	ON	ON	OFF	OFF	ON	ON	ON
1A	ON	ON	ON	OFF	OFF	ON	OFF	ON
1C	ON	ON	ON	OFF	OFF	OFF	ON	ON
1E	ON	ON	ON	OFF	OFF	OFF	OFF	ON
20	ON	ON	OFF	ON	ON	ON	ON	ON
22	ON	ON	OFF	ON	ON	ON	OFF	ON
24	ON	ON	OFF	ON	ON	OFF	ON	ON
26	ON	ON	OFF	ON	ON	OFF	OFF	ON
28	ON	ON	OFF	ON	OFF	ON	ON	ON
2A	ON	ON	OFF	ON	OFF	ON	OFF	ON
2C	ON	ON	OFF	ON	OFF	OFF	ON	ON
2E	ON	ON	OFF	ON	OFF	OFF	OFF	ON
30	ON	ON	OFF	OFF	ON	ON	ON	ON
32	ON	ON	OFF	OFF	ON	ON	OFF	ON
34	ON	ON	OFF	OFF	ON	OFF	ON	ON
36	ON	ON	OFF	OFF	ON	OFF	OFF	ON
38	ON	ON	OFF	OFF	OFF	ON	ON	ON
3A	ON	ON	OFF	OFF	OFF	ON	OFF	ON
3C	ON	ON	OFF	OFF	OFF	OFF	ON	ON
3E	ON	ON	OFF	OFF	OFF	OFF	OFF	ON

	SUB-CHANNEL ADDRESS SELECT SWITCH SW1							
ADDRESS	8	7	6	5	4	3	2	1
40	ON	OFF	ON	ON	ON	ON	ON	ON
42	ON	OFF	ON	ON	ON	ON	OFF	ON
44	ON	OFF	ON	ON	ON	OFF	ON	ON
46	ON	OFF	ON	ON	ON	OFF	OFF	ON
48	ON	OFF	ON	ON	OFF	ON	ON	ON
4A	ON	OFF	ON	ON	OFF	ON	OFF	ON
4C	ON	OFF	ON	ON	OFF	OFF	ON	ON
4E	ON	OFF	ON	ON	OFF	OFF	OFF	ON
50	ON	OFF	ON	OFF	ON	ON	ON	ON
52	ON	OFF	ON	OFF	ON	ON	OFF	ON
54	ON	OFF	ON	OFF	ON	OFF	ON	ON
56	ON	OFF	ON	OFF	ON	OFF	OFF	ON
58	ON	OFF	ON	OFF	OFF	ON	ON	ON
5A	ON	OFF	ON	OFF	OFF	ON	OFF	ON
5C	ON	OFF	ON	OFF	OFF	OFF	ON	ON
5E	ON	OFF	ON	OFF	OFF	OFF	OFF	ON
60	ON	OFF	OFF	ON	ON	ON	ON	ON
62	ON	OFF	OFF	ON	ON	ON	OFF	ON
64	ON	OFF	OFF	ON	ON	OFF	ON	ON
66	ON	OFF	OFF	ON	ON	OFF	OFF	ON
68	ON	OFF	OFF	ON	OFF	ON	ON	ON
6A	ON	OFF	OFF	ON	OFF	ON	OFF	ON
6C	ON	OFF	OFF	ON	OFF	OFF	ON	ON
6E	ON	OFF	OFF	ON	OFF	OFF	OFF	ON
70	ON	OFF	OFF	OFF	ON	ON	ON	ON
72	ON	OFF	OFF	OFF	ON	ON	OFF	ON
74	ON	OFF	OFF	OFF	ON	OFF	ON	ON
76	ON	OFF	OFF	OFF	ON	OFF	OFF	ON
78	ON	OFF	OFF	OFF	OFF	ON	ON	ON
7A	ON	OFF	OFF	OFF	OFF	ON	OFF	ON
7C	ON	OFF	OFF	OFF	OFF	OFF	ON	ON
7E	ON	OFF	OFF	OFF	OFF	OFF	OFF	ON

	SUB-CHANNEL ADDRESS SELECT SWITCH SW1							
ADDRESS	8	7	6	5	4	3	2	1
80	OFF	ON	ON	ON	ON	ON	ON	ON
82	OFF	ON	ON	ON	ON	ON	OFF	ON
84	OFF	ON	ON	ON	ON	OFF	ON	ON
86	OFF	ON	ON	ON	ON	OFF	OFF	ON
88	OFF	ON	ON	ON	OFF	ON	ON	ON
8A	OFF	ON	ON	ON	OFF	ON	OFF	ON
8C	OFF	ON	ON	ON	OFF	OFF	ON	ON
8E	OFF	ON	ON	ON	OFF	OFF	OFF	ON
90	OFF	ON	ON	OFF	ON	ON	ON	ON
92	OFF	ON	ON	OFF	ON	ON	OFF	ON
94	OFF	ON	ON	OFF	ON	OFF	ON	ON
96	OFF	ON	ON	OFF	ON	OFF	OFF	ON
98	OFF	ON	ON	OFF	OFF	ON	ON	ON
9A	OFF	ON	ON	OFF	OFF	ON	OFF	ON
9C	OFF	ON	ON	OFF	OFF	OFF	ON	ON
9E	OFF	ON	ON	OFF	OFF	OFF	OFF	ON
A0	OFF	ON	OFF	ON	ON	ON	ON	ON
A2	OFF	ON	OFF	ON	ON	ON	OFF	ON
A4	OFF	ON	OFF	ON	ON	OFF	ON	ON
A6	OFF	ON	OFF	ON	ON	OFF	OFF	ON
A8	OFF	ON	OFF	ON	OFF	ON	ON	ON
AA	OFF	ON	OFF	ON	OFF	ON	OFF	ON
AC	OFF	ON	OFF	ON	OFF	OFF	ON	ON
AE	OFF	ON	OFF	ON	OFF	OFF	OFF	ON
B0	OFF	ON	OFF	OFF	ON	ON	ON	ON
B2	OFF	ON	OFF	OFF	ON	ON	OFF	ON
B4	OFF	ON	OFF	OFF	ON	OFF	ON	ON
B6	OFF	ON	OFF	OFF	ON	OFF	OFF	ON
B8	OFF	ON	OFF	OFF	OFF	ON	ON	ON
BA	OFF	ON	OFF	OFF	OFF	ON	OFF	ON
BC	OFF	ON	OFF	OFF	OFF	OFF	ON	ON
BE	OFF	ON	OFF	OFF	OFF	OFF	OFF	ON

	SUB-CHANNEL ADDRESS SELECT SWITCH SW1							
ADDRESS	8	7	6	5	4	3	2	1
C0	OFF	OFF	ON	ON	ON	ON	ON	ON
C2	OFF	OFF	ON	ON	ON	ON	OFF	ON
C4	OFF	OFF	ON	ON	ON	OFF	ON	ON
C6	OFF	OFF	ON	ON	ON	OFF	OFF	ON
C8	OFF	OFF	ON	ON	OFF	ON	ON	ON
CA	OFF	OFF	ON	ON	OFF	ON	OFF	ON
CC	OFF	OFF	ON	ON	OFF	OFF	ON	ON
CE	OFF	OFF	ON	ON	OFF	OFF	OFF	ON
D0	OFF	OFF	ON	OFF	ON	ON	ON	ON
D2	OFF	OFF	ON	OFF	ON	ON	OFF	ON
D4	OFF	OFF	ON	OFF	ON	OFF	ON	ON
D6	OFF	OFF	ON	OFF	ON	OFF	OFF	ON
D8	OFF	OFF	ON	OFF	OFF	ON	ON	ON
DA	OFF	OFF	ON	OFF	OFF	ON	OFF	ON
DC	OFF	OFF	ON	OFF	OFF	OFF	ON	ON
DE	OFF	OFF	ON	OFF	OFF	OFF	OFF	ON
E0	OFF	OFF	OFF	ON	ON	ON	ON	ON
E2	OFF	OFF	OFF	ON	ON	ON	OFF	ON
E4	OFF	OFF	OFF	ON	ON	OFF	ON	ON
E6	OFF	OFF	OFF	ON	ON	OFF	OFF	ON
E8	OFF	OFF	OFF	ON	OFF	ON	ON	ON
EA	OFF	OFF	OFF	ON	OFF	ON	OFF	ON
EC	OFF	OFF	OFF	ON	OFF	OFF	ON	ON
EE	OFF	OFF	OFF	ON	OFF	OFF	OFF	ON
F0	OFF	OFF	OFF	OFF	ON	ON	ON	ON
F2	OFF	OFF	OFF	OFF	ON	ON	OFF	ON
F4	OFF	OFF	OFF	OFF	ON	OFF	ON	ON
F6	OFF	OFF	OFF	OFF	ON	OFF	OFF	ON
F8	OFF	OFF	OFF	OFF	OFF	ON	ON	ON
FA	OFF	OFF	OFF	OFF	OFF	ON	OFF	ON
FC	OFF	OFF	OFF	OFF	OFF	OFF	ON	ON
FE	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON

6.3.3.2 Control Unit Selection Prioritization and Propagation

Control Unit selection is controlled by Select Out, Select In and Hold Out. Select Out and Select In form a loop; the Select Out signal passes from the channel through each Control Unit to the cable terminator block. It is then returned through each Control Unit back to the channel as Select In. Most Control Unit selection circuitry can be attached to either Select Out or Select In. A selection priority is established because the rise of Select Out is effective only to the first Control Unit on the line. If the selection is not required, the signal is propagated by each Control Unit to the next on the line. This priority is in descending sequence from the channel through each Control Unit with selection circuitry attached to Select Out. Thereafter, any Control Units with selection circuitry attached to Select In can be selected in descending order, back to the channel.

The HSM does not have a priority jumpering option and always selects on the rise of Select Out. In IBM terminology this is "High Priority" selection. The HSM channel priority depends only on its position in the cable daisy-chain. The user provides the channel cables to the HSM, and therefore chooses their lengths and positions, which depend on the physical and logical locations of the HSM.

When the HSM is powered-down or switched offline, selection propagation is achieved through a relay.

The maximum channel cable length between the Host and the HSM is 200 feet. In addition, each additional Control Unit between the Host and the HSM subtracts 15 feet from this maximum. For example, if two control units are positioned between the Host and the HSM, the maximum cable length is 170 feet.

6.3.4 Channel Interface

The channel interface is a set of lines over which the HSM and the Host system channel exchange control and data signals. All standard channel sequences are supported with the exception of Streaming and High-Speed sequences.

6.3.4.1 Bus Lines

Each bus is a set of nine lines consisting of eight information lines and one parity line. Information on the bus is arranged so that bit position 7 always carries the low-order bit within an eight-bit byte. The parity bit is used to ensure the byte on any bus always has odd parity.

6.3.4.2 Bus Out Lines

Bus Out is used to transmit addresses, commands, control instructions and data from the host channel to the HSM. The type of information transmitted over Bus Out is indicated by the outbound Tag lines.

- When Address Out is up during the channel-initiated selection sequence, Bus Out specifies the address of the HSM with which the channel is to communicate
- When Command Out is up in response to Address In during the channel-initiated selection sequence, Bus Out specifies a command.
- When Service Out is up in response to Service In during the execution of a Write command, Bus Out contains data to be processed by the HSM.

6.3.4.3 Bus In Lines

Bus In is used to transmit addresses, status, sense information and data from the HSM to the Host channel. The type of information transmitted over the Bus In lines is indicated by the inbound Tag lines.

- When Address In is up on a Control Unit initiated selection sequence, Bus In specifies the address of the selected HSM.
- When Status In is up, Bus In contains a byte of information that describes the status of the HSM.
- When Service In is up during the execution of a Read or Sense command, the information depends on the type of operation. During a read operation, the bus contains response data from the HSM. During a Sense operation, the bus contains a set of bits describing in more detail the status of the HSM and the conditions under which the last operation terminated.

6.3.4.4 Tag Lines

The Tag lines are used for interlocking and controlling the information on the buses, and for any special sequences.

The seven Tag lines used by the channel interface are:

Address Out, Address In, Command Out, Status In, Service Out, Service In, and Disconnect In.

6.3.4.5 Selection Control Lines

The Selection Control lines are used for scanning or the selection of the attached control units (HSMs).

The seven Selection Control lines used by the channel are:

Operational Out, Operational In, Hold Out, Select Out, Select In, Suppress Out and Request In.

6.3.4.6 Metering Control Lines

The three Metering control lines, Meter Out, Meter In and Clock Out are not used by the HSM. These lines are normally used for usage meters located on control units and to condition enable/disable switches which are not implemented on the HSM.

6.4 SDLC Emulation

The HSM is viewed by the Host as a DCE (data communications equipment) operating as a nonswitched point-to-point half duplex device, and the electrical interface conforms to the RS-449 standard without the secondary channel.

The following are configurable options:

- The message header length (1 to 255 characters).
- The character set can be either EBCDIC or ASCII.
- The station address.
- The baud rate can be selected.

The word format is NOT configurable.

6.4.1 Message Header Length

Each transaction to the HSM begins with a string of characters (header) which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 255; the default value is 4.

6.4.2 Station Address

The station address is the address of the secondary station (in this case the HSM). This address must be the same as defined in Host application software. The default address is X'40.

6.4.3 Setting the Jumpers for DCE Operation

The RS-449 Host interface must be configured as a DCE port. The applicable jumpers are inserted on a row of pins JPR3, JPR4 and JPR5 on the SDLC Interface board (see Figure 3.6 and Figure 3.7).

JPR2 provides connections to earth for the cable shield and the signal ground, which may be required by the system, but are not normally used.

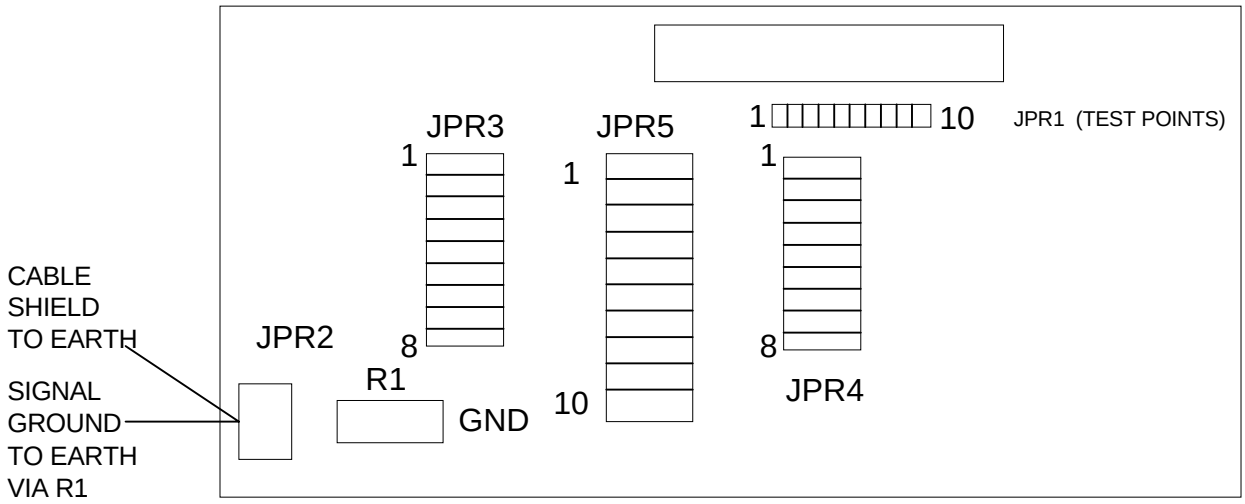


Figure 3.6- SDLC Interface Board

Disconnect power before fitting or removing the jumpers. For access see Chapter 2.

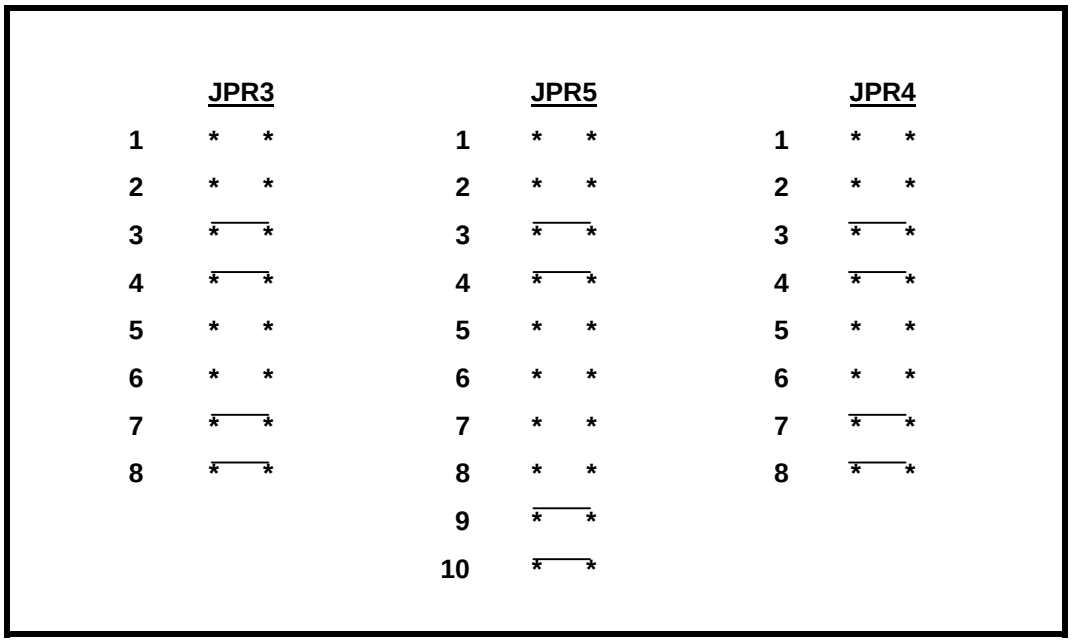


Figure 3.7- The Jumpers on the SDLC Interface Board for DCE Operation

6.4.4 Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key into the rear panel KEY switch, and rotate it clockwise a quarter turn then allow it to spring back), with power applied and the Console connected.

The Console displays:

HSM going OFFLINE, press Reset to go Online.

Master Key loading facilities now available.

Offline>

Enter CH < Return > (Configure Host) to initiate the set-up dialogue. Examples of the various SDLC configurations are described in the following paragraphs. User inputs are shown underlined.

6.4.4.1 ASCII Character set

In the example, the ASCII character set is selected, the message header is 8 characters and the station address is set to X'40 (default value). The baud is changed to 224000 (default value).

Example:
Offline> CH < Return >

Message header length (1-255): 8
Asynchronous/Bisynchronous 3270/SDLC (A/B/S): S
EBCDIC/ASCII (E/A): A
Station address (2 hex): 40

BAUD RATES

1. 9600
2. 19200
3. 38400
4. 56000
5. 64000
6. 112000
7. 224000
8. 246000 (256000 for RG7310)

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 5) 7 < Return >

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.4.4.2 EBCDIC Character Set

In the example, the EBCDIC character set is selected, the message header is 8 characters and the station address is set to X'40 (default value). The baud is not changed from 224000 (default value).

Example:

Offline> CH < Return >

Message header length (1-255): 8
Asynchronous/Bisynchronous 3270/SDLC (A/B/S): S
EBCDIC/ASCII (E/A): E
Station address (2 hex): 40

BAUD RATES

1. 9600
2. 19200
3. 38400
4. 56000
5. 64000
6. 112000
7. 224000
8. 246000 (256000 for RG7310)

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 7) < Return >

After completing the procedure reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.5 SNA-SDLC Synchronous Emulation

The SNA-SDLC interface in the HSM emulates a 3274 Control Unit (CU) with a single device attached. At the SNA level, this control unit appears as two Network Addressable Units (NAU); a Physical Unit (PU) and a Logical Unit (LU). A standard 3274 CU contains 32 such LUs.

The electrical interface between the Host and the HSM conforms to either the RS-232-C standard or the V.35 standard (if fitted).

The following are configurable options available in the SNA-SDLC environment:

- The message header length (1 to 100 characters).
- A "Transparent" Data mode can be selected.
- The HSM can support the IBM IMS and CICS environments.
- The Host interface can be either DCE or DTE.
- The Host interface can be through either the RS-232-C or V.35 port.
- The baud rate can be selected (if DCE).
- The SDLC Station Address.

6.5.1 Command Message Format

When the SNA-SDLC mode is selected, the standard HSM command/response message, as defined in the Programming Manual, is invalid. In an SDLC environment, the use of the start and end of text characters, STX and ETX, is not relevant, and they are omitted from all messages. Messages therefore start with the Message Header and end with either the last data element or the Message Trailer if it is present.

6.5.2 Message Header Length

Each transaction to the HSM begins with a string of characters which the Host can use to identify the transaction (or for any other purpose). The HSM returns the string unchanged to the Host in the response message. The length of the header can be set to any value between 1 and 100; the default value is 4.

6.5.3 Transparent Data Mode

If the "Normal" (default) setting is selected, the HSM scans each incoming message for any 3270 "Orders". When such an Order is found it is removed from the message and the HSM proceeds to process the message as normal.
If the "Transparent" setting is selected, 3270 Order removal is not carried out, and it is the responsibility of the Host system to ensure that 3270 Orders do not appear in the data sent to the HSM. Hence, in transparent data mode, the messages sent to the HSM can contain binary data.

6.5.4 Character Set

On selection of the SNA-SDLC option, the HSM defaults to the EBCDIC set. This setting can be over-ridden by the character set selected in the SNA session Bind.

6.5.5 Host Environment

The HSM can be made compatible with an IBM Host running applications under IMS or CICS.

6.5.5.1 IMS

In IMS applications, the HSM requires the entry of one or more test strings to enable it to distinguish between valid transactions and system error and status messages. When the Host software is written, the programmer must insert one of the test strings in the message header field of each valid transaction to the HSM.

The HSM searches for the strings and accepts a transaction only if it contains one of them. It allows a maximum of 20 characters (including delimiters) to be entered. The strings, delimited by commas, can contain any alphanumeric character, and do not need to be the same length. If more than one string is defined, the HSM accepts a transaction if it matches any one of them.

In addition, a test string offset is required. This value allows the test string to be placed at any fixed position in the message header, by specifying the number of characters to skip before the comparison is made. It can be any value from zero to the message header length (but if the header length minus the offset is less than the length of a test string, that particular string will never be found).

All messages that do not have one of the test strings at the defined offset are ignored, and the HSM responds with a PA2 AID at the next poll.

6.5.5.2 CICS

In CICS applications, the HSM searches the beginning of each transaction for the DFH string, which identifies all CICS system messages. If it is found, the message is ignored and the HSM responds with the CLEAR AID at the next poll.

6.5.6 SDLC Station Address

The station address is the address of the secondary station (in this case the HSM). This address must be the same as defined in the Host system configuration. The default address is X'C1.

6.5.7 Baud Rate and Word Format

The baud rate is configurable only when the DCE option is selected. The word format is preset to: no parity, 8 data bits, 1 stop bit, when SNA-SDLC mode is selected.

6.5.8 Defining the RS-232-C Host Port

For DCE or DTE operation, the applicable jumpers are inserted on a row of pins, JPR5, on the Processor circuit board (see Figure 3.1and Figure 3.8). The equipment is shipped from the factory configured for DCE emulation.

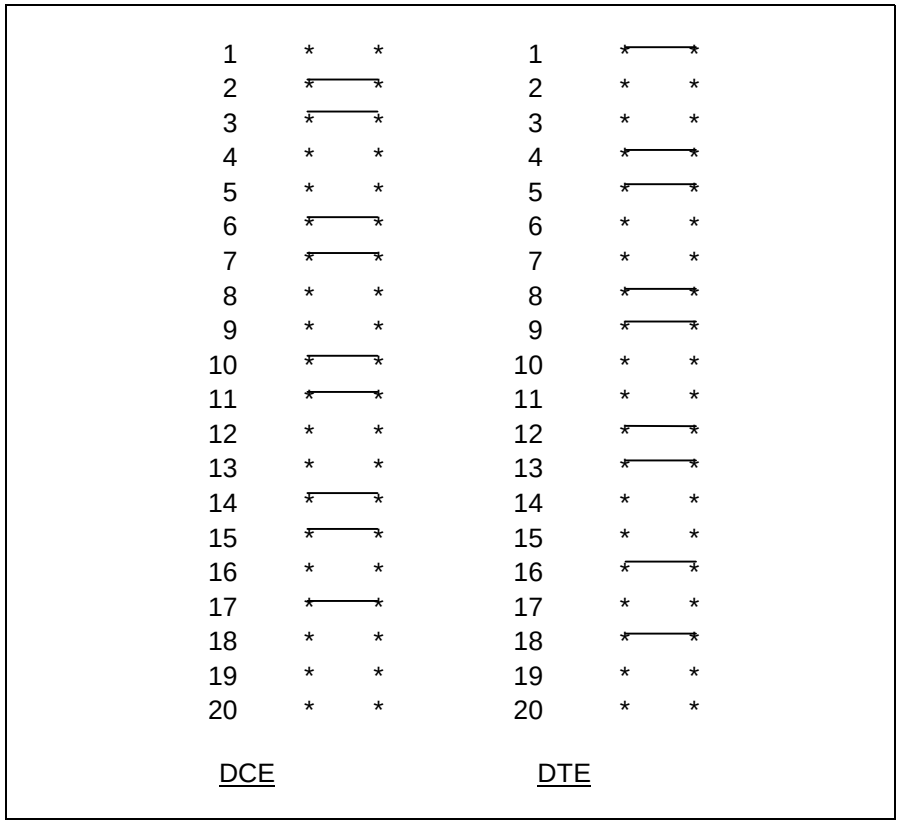


Figure 3.8 – The Jumpers onJPR5 for DCE or DTE(RS-232-CPort)

Disconnect power before fitting or removing the jumpers. For access see Chapter 2. The required options must also be selected during the software configuration process.

6.5.9 Defining the V.35 Host Port

The V.35 Interface circuit board, which contains the V.35 Host port, is located above the RS-232-C Host port on the rear panel. The 34-pin V.35 Host port can be configured to be either a DCE or a DTE, by inserting the applicable jumpers on four rows of pins JPR1, JPR2, JPR3 and JPR4 (see Figure 3.9and Figure 3.10). The equipment is shipped from the factory configured for DCE emulation.

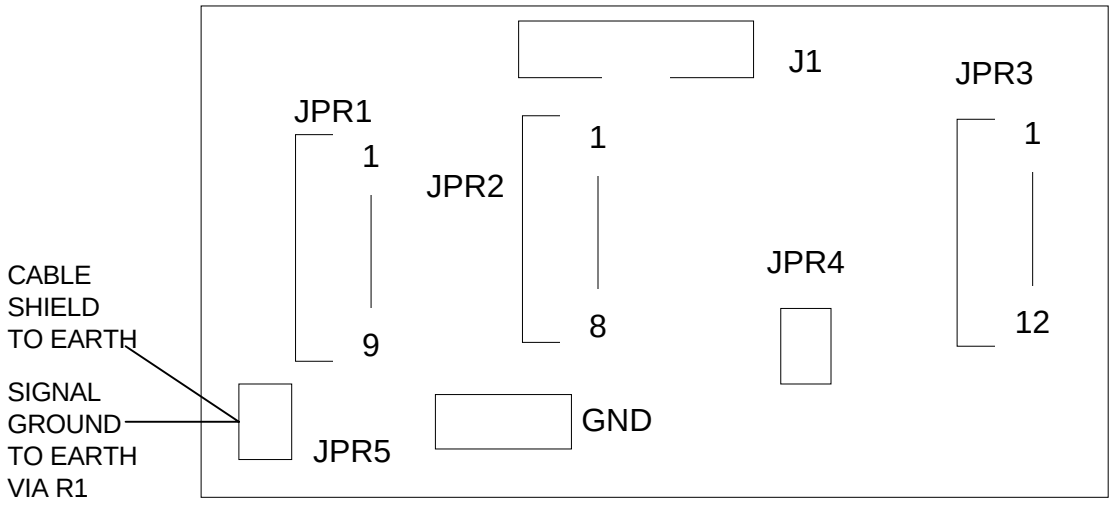


Figure 3.9– V35 Interface Circuit Board

JPR5 provides connections to earth for the cable shield and the signal ground, which may be required by the system, but are not normally used.

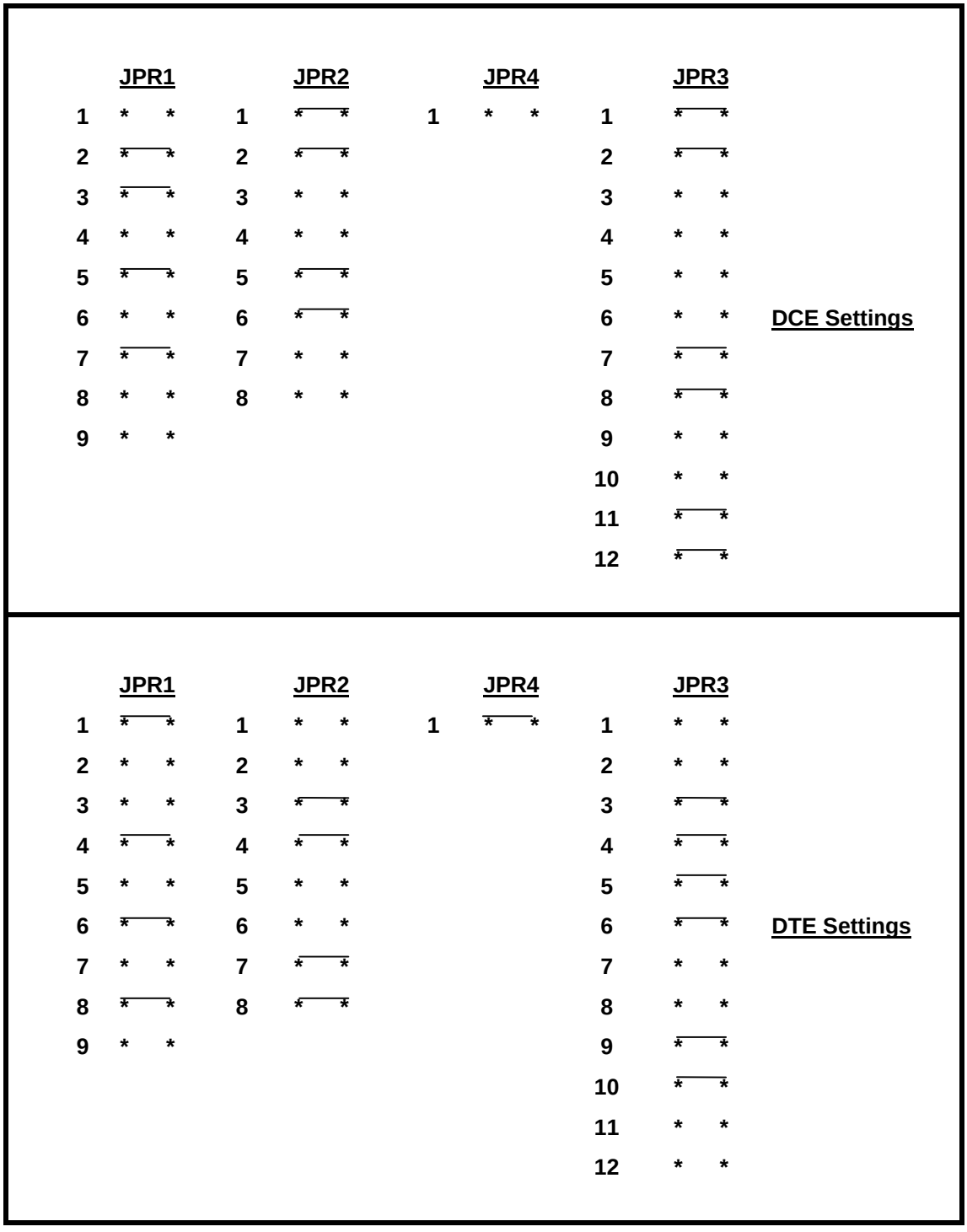


Figure 3.10 - The Jumpers on the V.35 Interface Board for DCE or DTE

Disconnect power before fitting or removing the jumpers. For access see Chapter 2. The required options must also be selected during the software configuration process.

6.5.10 Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key into the rear panel KEY switch, and rotate it clockwise a quarter turn then allow it to spring back), with power applied and the Console connected.

The Console displays:

HSM going OFFLINE, press Reset to go Online.

Master Key loading facilities now available.

Offline>

Enter CH < Return > (Configure Host) to initiate the set-up dialogue. Examples of the various SNA-SDLC configurations are described in the following paragraphs. User inputs are shown underlined.

6.5.10.1 No IMS or CICS, DCE, RS-232-C Interface

In the example, neither IMS nor CICS support is selected. The V.35 interface is fitted. The HSM is a configured as a DCE (Data Communications Equipment) (i.e., the HSM supplies the Clock signal for the RS-232-C interface). The Host baud is changed to 19200 bps.
Example:

Offline> CH < Return >

Message header length (1-100): 4
Asynchronous/SNA-SDLC 3274 (A/S): S
Transparent Mode (Y/N): N
Station Address (2 hex): C1
IMS/CICS/General (I/C/G): G
DTE/DCE (T/C): C
RS232 or V.35(R/V): R (This prompt is omitted for the RG7500 where the V.35 interface is not fitted).

BAUD RATES

1. 9600
2. 19200
3. 38400
4. 56000
5. 64000

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 1) 2 < Return >

After completing the procedure reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.5.10.2 IMS Support, DCE, V.35 Interface

In the example, IMS support is selected and the HSM is configured for DCE. The V.35 interface is fitted. The V.35 interface is selected for all Host communications. The Host baud is changed to 56000 bps.

Example:

Offline> CH < Return >

Message header length (1-100): 20
Asynchronous/SNA-SDLC 3274 (A/S): S
Transparent Mode (Y/N): N
Station Address (2 hex): C1
IMS/CICS/General (I/C/G): I
IMS message identifier (1-20): PIN,MAC
Identifier offset: 3
DTE/DCE (T/C): C
RS232 or V.35 (R/V): V (This prompt is omitted for the RG7500 where the V.35 interface is not fitted).

BAUD RATES

1. 9600
2. 19200
3. 38400
4. 56000
5. 64000

In response to the prompts, enter the number of the desired option or < RETURN > for no change.

Host baud rate: (current value = 2) 4 < Return >

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.5.10.3 CICS Support, DTE, V.35 Interface

In the example, CICS support is selected. The V.35 interface is fitted. The HSM is configured as a DTE (Data Terminal Equipment) and depends on the Host for the Clock signal on the V.35 interface. The Host baud rate cannot be set. No selection for Transparent mode or Station Address is offered, so they default to NO and C1.

Example:

Offline> CH < Return >

Message header length (1-100): 4
Asynchronous/SNA-SDLC 3274 (A/S): S
Transparent Mode (Y/N):
Station Address (2 hex):
IMS/CICS/General (I/C/G): C
DTE/DCE (T/C): T
RS232 or V.35 (R/V): V (This prompt is omitted for the RG7500 where the V.35 interface is not fitted).

After completing the procedure, reset the HSM: press then release the RESET button on its rear panel. The new values do not take effect until this has been done.

6.6 Ethernet

6.6.1 Configuring the Hardware

The HSM can be set to use either Ethernet interface 10base2 or 10base5. The 15-way D-type 10Base5 connector on the rear of the HSM is always active. The BNC 10Base2 connector is active only when the link is made on jumper JPR1 on the Ethernet circuit board (see Figure 3.11). Do NOT connect to both. **(The JPR1 link should not be made unless the 10base2 connection is to be used)**. The board is mounted vertically on the rear panel of the HSM.

10baseT using RJ45 type connectors can be achieved by the use of an AUI to 10baseT converter.

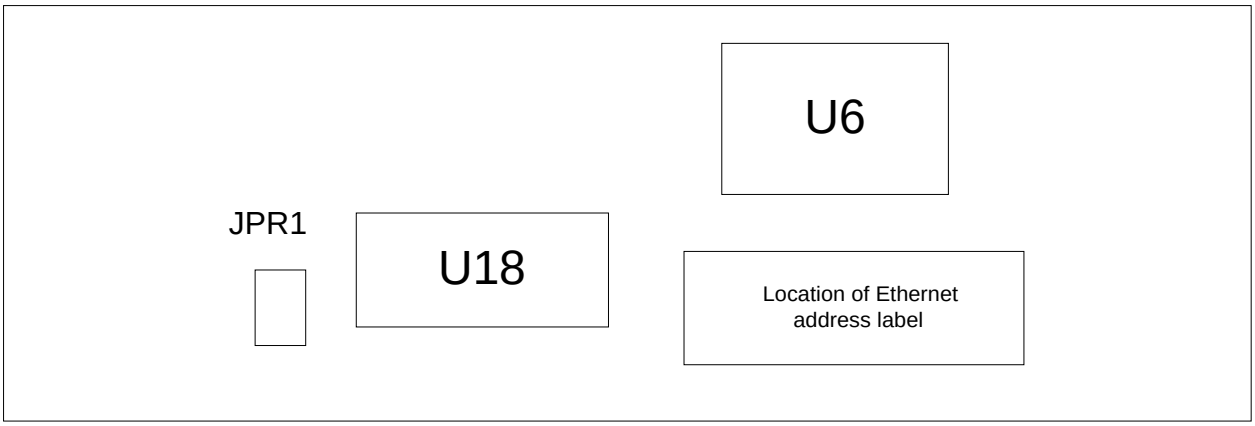


Figure 3.11 - Ethernet Circuit Board

Disconnect power before fitting or removing the jumper. For access see Chapter 2.

6.6.2 Configuring the Software

To configure the Host port, set the HSM into the offline state (insert the key into the KEY switch on the rear panel, and rotate it clockwise a quarter turn, then allow it to spring back), with power applied and the Console connected. There are a number of prompts for configuring the software.

The message header length, the use of Ethernet, the character set either ASCII or EBCIDIC, the availability of a UDP port, the availability and number of TCP ports, the IP address, the Well-Known-Port address, the default gateway and the subnet mask.

The number of TCP/IP sockets available has a maximum of 8 but is reduced to 7 if UDP protocol is enabled.

The IP address is the Internet Protocol address of the unit in the system. It is four decimal numbers, each not exceeding 255_{10}.
The Well-Known-Port address is the publicised TCP Port address of the HSM, in the range 00000_{10} to 65535_{10} representing an address in the range 0000_{16} to $FFFF_{16}$.
The default gateway address is the Internet Protocol address of the default gateway in the system. It is four decimal numbers, each not exceeding 255_{10}.
The subnet mask is used to define the network class.
The addresses have no cold start defaults; if < Return > is entered after a prompt, the previously-configured address is used.
After completing the procedure, reset the HSM: press then release the RESET button on its rear panel.

UDP and TCP configurations are given in the following examples

6.6.2.1 UDP Configuration

Enter CH < Return > (Configure Host), to initiate the set-up dialogue. Respond to the prompts:
Message header length (1-255): 4
Async or Ethernet? [A/E]: E
EBCDIC/ASCII [E/A]: A
Enter IP address: 128.100.3.1
Enter Well-Known-Port address: 01500
UDP [Y/N]: Y
TCP [Y/N]: N
Enter Default Gateway: 128.100.3.5
Enter Subnet mask: 255.255.255.000

To read the current configuration, enter QH < Return >.

The HSM shows:
Message header length: 04
Protocol: Ethernet
Character format: ASCII
IP address: 128.100.003.001
Well-Known-Port address: 01500
Protocol: UDP
Default gateway: 128.100.003.005
Subnet mask: 255.255.255.000

6.6.2.2 TCP/IP Configuration

Enter CH < Return > (Configure Host), to initiate the set-up dialogue. Respond to the prompts:
Message header length (1-255): 4
Async or Ethernet? [A/E]: E
EBCDIC/ASCII [E/A]: A
Enter IP address: 128.100.3.1
Enter Well-Known-Port address: 01500
UDP [Y/N]: N
TCP [Y/N]: Y
Number of connections [1 - 8]: 6
Enter Default Gateway: 128.100.3.5
Enter Subnet mask: 255.255.255.000

To read the current configuration, enter QH < Return >.

The HSM shows:
Message header length: 04
Protocol: Ethernet
Character format: ASCII
IP address: 128.100.003.001
Well-Known-Port address: 01500
Protocol: TCP, 6 Connections
Default gateway: 128.100.003.005
Subnet mask: 255.255.255.000

6.6.2.3 UDP and TCP/IP Configuration

Enter CH < Return > (Configure Host), to initiate the set-up dialogue. Respond to the prompts:
Message header length (1-255): 4
Async or Ethernet? [A/E]: E

EBCDIC/ASCII [E/A]: A
Enter IP address: 128.100.3.1
Enter Well-Known-Port address: 01500
UDP [Y/N]: Y
TCP [Y/N]: Y
Number of connections [1 - 7]: 6
Enter Default Gateway: 128.100.3.5
Enter Subnet mask: 255.255.255.000

To read the current configuration, enter QH < Return >.

The HSM shows:
Message header length: 04
Protocol: Ethernet
Character format: ASCII
IP address: 128.100.003.001
Well-Known-Port address: 01500
Protocol: UDP and TCP, 6 Connections
Default gateway: 128.100.003.005
Subnet mask: 255.255.255.000

7 PROGRAMMING GUIDE

7.1 Asynchronous Connected Option

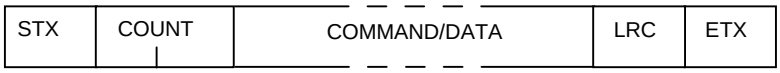
The HSM Asynchronous Connected mode operates as a communications attached device. It responds only to messages bracketed with STX and ETX (X'02 and X'03).

7.2 Transparent Asynchronous Connected Option

In the standard asynchronous mode of communication, codes like STX (X'02) and ETX (X'03) have a special meaning, but they can sometimes occur in a stream of binary data, where that special meaning does not apply.
To avoid ambiguity, Transparent Asynchronous Communications mode is used.

7.2.1 Sending Commands

The Host port of the HSM must be configured for Transparent Async Communications and 8-bit data transfers. The message format for Transparent Async Communications is:



Where:

- STX is the Start of Text character (X'02).
- COUNT is a two-byte hexadecimal value in the range X'0003 to X'03FB inclusive, representing the number of bytes in the COMMAND/DATA field. The count excludes the STX, COUNT, LRC and ETX.
- LRC is a single-byte Longitudinal Redundancy Check character. It is calculated by performing an exclusive-OR on each byte of the data sent over the communications link excluding the STX, COUNT, LRC and the ETX.
- ETX is the End of Text character (X'03).

7.2.2 HSM Processing of Packets

When the HSM receives a Transparent Async packet it:

- Checks the LRC value with that computed over the input data and returns a response message with Error 91 if a match is not obtained.
- Checks that the Count value is between limits. If this check fails, the HSM responds in one of two ways:

If Count > X'03FB,

it returns a response message with Error 92;
otherwise it responds with the following error message:
Message Header : 0000
Response Code : ZZ
Error Code : 92

e.g., for Message Header length 4, the response is 0000ZZ92.

- Checks that the number of characters received between the Count characters and the LRC matches the value in Count. If this check fails, it returns a response message with Error 92.
- If no errors are discovered in the Transparent Async packet, the HSM processes the command and responds accordingly.

If the HSM discovers both errors (Error 91 and Error 92), it reports Error 92.

7.2.3 Parity Errors

If the HSM reports Error 90 there is a Data Parity Error. Check the HSM Host port settings using the QH Console command and ensure that the correct parity is in use.

7.3 Bisynchronous Connected Option

The HSM Bisynchronous Connected mode emulates a 3270 Control Unit with one terminal attached. It operates with Polls and Selects; commands are bracketed with STX and ETX. Programming examples are shown in Appendix A.

7.4 Channel Attach Option

The HSM Channel Attach option emulates a standard tape control. The application programmer need only use Open, Write, Read and Close commands.
When the HSM is defined as a tape control unit, ensure that the Job Control Language (JCL) is using the following parameters:

- Bypass Label Processing (LABEL=BLP).
- Undefined Record Format (RECFM=U).
- Block size less than 1020 bytes.

Most transactions require less than 100 milliseconds of internal processing time, so timeouts should not be a problem. (The longest transaction takes approximately three seconds.) However, if the HSM goes down it may not respond to the Host, so a timeout is useful. (IODEVICE MACRO, TIMEOUT=Y is the default).

All Write commands to the HSM must be followed by a Read command. This protocol guarantees that the Host receives a response to any transaction initiated, and eliminates any polling sequence by the Host. Whenever the HSM is opened and as part of any channel I/O error recovery, the application program should do a Read operation to ensure that the required "Write/Read" synchronisation is achieved. To prevent hang-ups on the channel, the HSM discards any Write data not preceded by a Read operation.

The Channel-Attach equipment does not use the STX and ETX (X'02' and X'03') characters that other versions of the HSM use to bracket each transaction.

Data in Host messages to the HSM are character data for the majority of commands. For all the standard commands, the HSM expects to see character data. Any binary value may be used in the message header and echoback field EXCEPT X'03'. This is used as an internal "end-of-record" indicator and should never be sent by the Host in the standard commands.

The Channel-Attach equipment returns only one response for every print command (not two, as used by other versions of the HSM).

7.4.1 IOGEN Considerations

The HSM uses only one sub-channel address, and that address must be even (e.g. 0,2,4,... X'FC', X'FE').

The HSM emulates a basic magnetic tape and control unit, it is recommended that the HSM is configured as a dummy device a sample definition is shown in Appendix C.

7.4.2 HSM Channel Commands and Operation

The HSM supports the following five commands: WRITE, READ, NO OPERATION, SENSE and TEST I/O. Provided the command set is limited to these five commands. Use of any other channel commands in this mode may produce unpredictable results which could jeopardise the manufacturer's ability to support the device.

The following is a description of the commands supported by the HSM and the responses it generates.

7.4.2.1 Test I/O X'00'

The Test I/O command solicits the current status of the HSM specified by the address issued during the initial selection sequence.

If the channel card is not busy, the status byte presented indicates that the addressed HSM is ready for operation or is presenting status stacked from a previous operation. The status is cleared when it is accepted by the Host.

7.4.2.2 Write X'01', Read X'02'

To guarantee that the Host receives a response to any transaction it has sent to the HSM, a Read command must follow every Write command to the HSM. This protocol eliminates polling by the Host. Whenever the HSM is "opened" and as part of any channel I/O error recovery, the application program should issue a Read command to ensure that the required "Write/Read" synchronisation is achieved. To prevent hang-ups on the channel, the HSM discards any Write data if this command had not been preceded by a Read. If no data is available (either there has been no prior Write, or a Write produced no response data), the HSM returns the following ten bytes:

X'4C53', X'0004', X'0001', X'0000', X'0000'

When a Write command is issued from the host, the HSM presents Channel End status only in its ending status after all the data has been transferred. At this point, the Write operation is not completed and the channel has disconnected from the HSM. When the data received on this Write operation has been internally processed by the HSM, the response to this transaction is stored in the channel card buffer ready to be transferred to the host. The HSM reconnects to the channel by raising the Request In line, and presents Device End status during the initial selection sequence. This terminates the Write operation and disconnects from the channel. On the subsequent Read command, the data is transferred to the Host. Channel End and Device End are presented as ending status to this operation.

7.4.2.3 No Operation X'03'

The No Operation (NOP) command performs no function, does not transfer any data and does not disturb sense data information. Channel End and Device End are presented during the initial status presentation.

7.4.2.4 Sense X'04'

The Sense command is normally issued after the HSM has presented Unit Check status and the Host requests sense data. The Sense command causes the HSM to transmit up to 24 sense bytes to the Host. Byte 0 is the only one that has any significance. Byte 1 is always X'44' and byte 2 is X'03'. The other bytes, 3 to 23, are always X'00'. The bit position in byte 0 reflects the conditions present in the HSM at the time the Sense command is issued. The sense information stored in the HSM is reset by System Reset, Selective Reset and the acceptance of any Read or Write command. Channel End and Device End status are presented in the ending status on termination of the Sense command operation.

7.4.3 Unit Status and Sense Information

7.4.3.1 HSM Status Byte

The HSM initial status byte is sent to the channel as part of the initial selection sequence. When the channel accepts the initial status byte, the initial selection is completed. If the HSM issues an initial status byte of X'00', command execution begins automatically.

Bit	Designation	Interpretation
0	Attention	Not used
1	Status Modifier	Not used
2	Control Unit End (CUE)	The HSM is available for another operation. Set at the completion of any operation during which busy was signaled.
3	Busy	The HSM cannot execute a command owing to a pending interrupt or it is currently occupied with a previously initiated operation.
4	Channel End (CE)	The channel is no longer required for the operation.
5	Device End (DE)	Set on termination of all HSM commands.
6	Unit Check (UC)	The HSM has encountered an unusual condition. The cause of the unit check is stored as sense data, which is available to the program in response to a Sense command. Unit check is set when any sense byte 0 bit is set.
7	Unit Exception (UE)	Not used

7.4.3.2 Sense Information

The only sense bytes containing pertinent information are bytes 0 and 1. Because the HSM is primarily emulating a tape control unit, the sense data reflects that emulation.

Sense Byte	Sense Data	Interpretation
0	00	No error indicated/initialized value.
1	48	Ready and at load point.
0	80	Command reject/an invalid command was sent.
1	48	Ready and at load point.
0	40	Intervention required/channel buffer not available.
1	48	Ready and at load point.
0	40	Intervention required/response code reject rewind, unload CMD.
1	20	Not ready, or rewinding.
0	20	Bus Out check/HSM detected bad parity from the channel.
1	48	Ready and at load point.
5	40	3803/3420 Subsystem.
6	25	Capable of 800/1600 BPI; 200 IPS (mod 7).

All other sense bytes remain unchanged 00.

7.4.4 Sample Test Program

A sample test program to verify successful IOGEN and device connection to the Host is available from local support office.

7.5 SNA-SDLC Connected Option

This section details the 3274 Control Unit (CU) SNA-SDLC emulation provided in the HSM. It provides an architectural overview and a description of the SNA commands supported.

See also the following IBM publications:

3274 Control Unit Description and Programmer's Guide, No. GA23-0061-2.
SNA Format and Protocol Reference Manual: Architectural Logic,
No. SC30-3112-2.
IBM Synchronous Data Link Control - General Information, No. GA27-3093-2.

7.5.1 Session Components

From an SNA perspective, the HSM appears as two Network Addressable Units (NAU): the Physical Unit (PU) and a Logical Unit (LU). The HSM contains only one LU; a standard 3274 Control Unit (CU) contains up to 32.

Communications within SNA occurs in sessions, or logical relationships between NAUs. The Primary Logical Unit (PLU) is always the Host program; the HSM contains the Secondary Logical Unit (SLU) in all LU-LU sessions. The System Service Control Point (SSCP) resides in the communications Front End Processor (FEP) for SDLC CUs; it manages the active sessions between the HSM and the Host.

The HSM supports three concurrent sessions:
SSCP - PU (access method - HSM PU).
SSCP - SLU (access method - HSM SLU).
PLU - SLU (Host program - HSM SLU).

7.5.2 Supported Commands

The table lists the SNA commands the HSM supports and the sessions in which each is valid.

SNA Command		Session Type		
Name	**Type**	**SSCP-PU**	**SSCP-SLU**	**PLU-SLU**
ACTPU	SC	To HSM		
DACTPU	SC	To HSM		
ACTLU	SC		To HSM	
DACTLU	SC		To HSM	
Bind	SC			To HSM
Unbind	SC			To HSM
SDT	SC			To HSM
Clear	SC			To HSM
Cancel	DFC			To HSM
Chase	DFC			To HSM
LUSTAT	DFC			To HSM
SHUTD	DFC			To HSM
SHUTC	DFC			From HSM
Bid	DFC			To HSM
Signal	DFC			To & From HSM
REQMS	FMD	To HSM		
RECFMS	FMD	From HSM		
Notify	FMD		From HSM	

7.5.3 Differences and Exceptions

An IBM 3274 CU contains up to 32 devices, the HSM emulation supports only device, 0. The SNA addresses are:

HSM PU Address = 0;
HSM LU Address = 2 (addresses 0 and 1 are reserved).

The SDLC Station Address is selectable, the default value is X'C1. Addresses X'00 and X'FF are reserved, all other CU address values are valid (i.e., X'01 to X'FE or 1 to 254).

The HSM does not implement the NMVT Alert and RTM commands.

Because the SLU in the HSM is the software, the PLU has the responsibility of initiating the logon.

7.5.4 Host SNA Session Considerations

7.5.4.1 Outbound Requests

Outbound FMD requests which carry FIC/OIC are expected to begin with a 3270 write-type command and a WCC. The COPY and WSF commands are not supported, and are rejected with sense code X'1003.

Only one HSM command can be sent outbound per chain; chain elements are concatenated in the HSM and the data is not given to the command processor until the LIC element is received.

7.5.4.2 Inbound Requests

Inbound reply requests which carry FIC/OIC always begin with the following sequence:

	EBCDIC	ASCII
AID: (‘Enter’)	X'7D	X'27
Cursor address:	X'40C1	X'2041
SBA order:	X'1140C1	X'112041

The HSM, unlike a true 3274, is strictly "speak-when-spoken-to". Therefore, when an FMD request that contains a valid HSM command is sent outbound, the HSM expects to return a reply FMD request inbound. This means that the Host request must leave the HSM in either CONTENTION or SEND state (by carrying either EB or CD).

If the HSM cannot return its reply because the Host left it in RCV state, it sends the DFC command ‘Signal' (X'00010000) to solicit a change of direction. The appropriate Host action is to send a null-RU or Write (with no data) request carrying EB or CD; the HSM then sends its pending reply. The HSM cannot buffer more than one reply, so if the Host request following an HSM-originated ‘Signal' contains an HSM command, the latter is discarded.

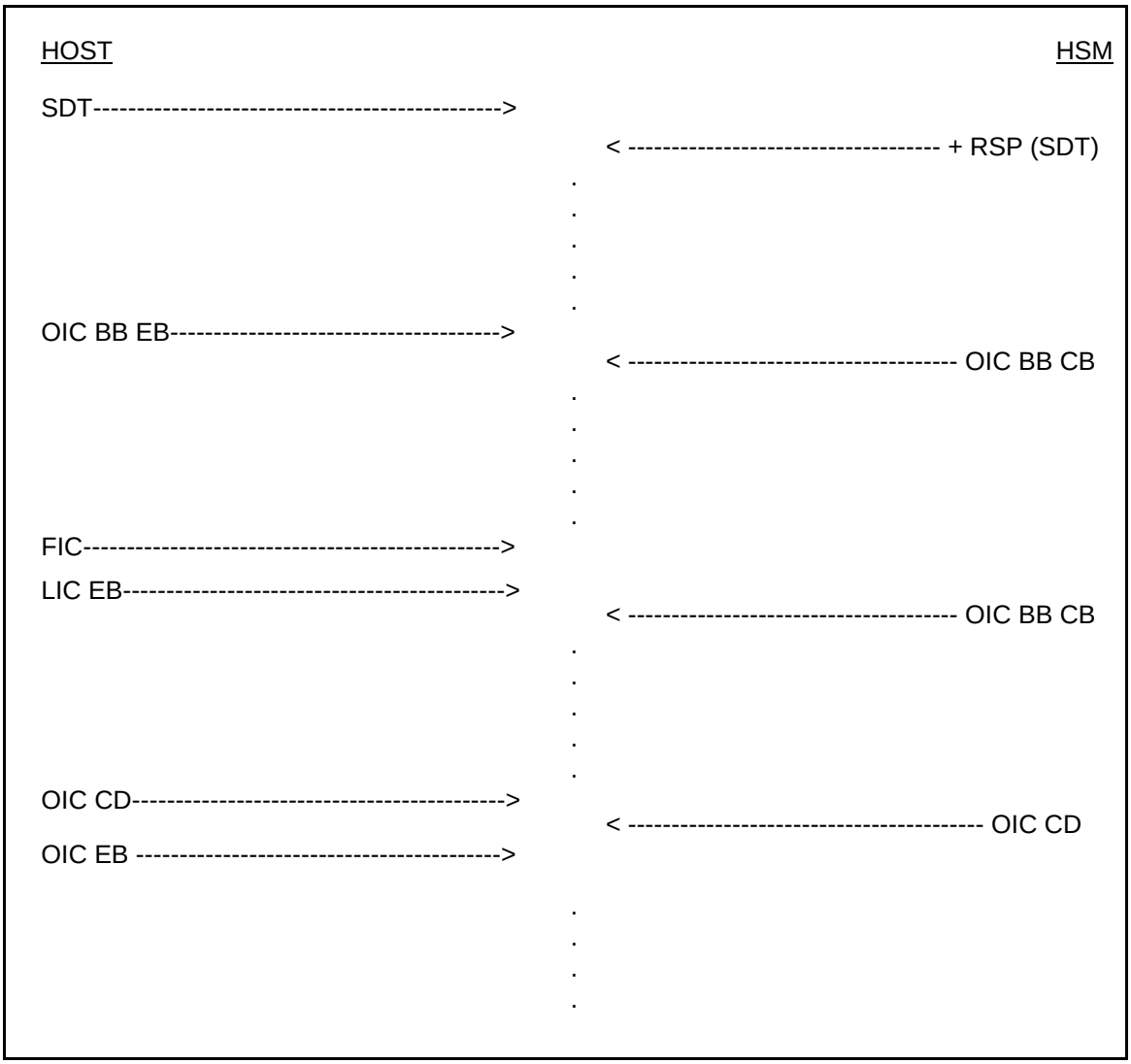


Figure 3.12 - SNA Command Sequences

Note that no BID was sent outbound in the example in Figure 3.20 . The HSM is, by convention, the contention winner. However, because it never sends unsolicited requests inbound, the Host can always begin a bracket if in the BETB state.

7.5.4.3 BIND Field Values

The table below shows suggested BIND field values. To maximise throughput, disable pacing and use Exception-response (RQE) whenever possible (the HSM always requests RQE if permitted by the BIND). The HSM does not support sending the Isolated Pacing Response (IPR), so, if primary-to-secondary pacing is required, the HSM must be bound for Definite-Response (RQD) on that half-session to allow the pacing response to be returned.

Byte Number	Hex Value	Comments
0	31	The Bind command.
1	01	Bind type and format.
2	03	Function management (FM) profile.
3	03	Transmission services (TS) profile.
4	B1	PLU can request single or multiple element RQD or RQE chains.
5	90	SLU can request single or multiple element RQE chains.
6	30	Selects EBCDIC code, the HSM supports the use of ASCII if bit 4 is set to one (X'38). This is a global setting, and affects all FMD requests that are character coded; the CSI bit in the RH is ignored.
7	80	Common protocols byte; Half duplex flip-flop (HDX FF), PLU does error recovery, HSM (3274) speaks first, data contention favors HSM (3274).
8	00	No secondary-to-primary pacing.
9	00	No primary-to-secondary pacing.
10	87	Maximum SLU RU size=1024. (Because of buffer constraints, the HSM never sends an RU greater than 996 bytes). If byte 10 is not accepted by the HSM, the bind is rejected with sense code X'0821.
11	87	Maximum PLU RU size=1024. (Because of buffer constraints, the Host should never send an RU greater than 988 bytes). If byte 11 is not accepted by the HSM, the bind is rejected with sense code X'0821.
12-n		All remaining bytes are ignored by the HSM.

7.5.4.4 Multiple RU Length Support

From HSM Functional Revision 5.03, the SND HSM accept any legal RU size from 256 and 1024 inclusive, on both inbound and outbound LU-LU half-sessions. This allows connection to IBM AS/400 minicomputers which do not allow the RU size to be changed in the Host and which require the RU size to be 256.

NOTE: HSM Functional Revisions prior to 5.03 accept only bytes 10 and 11 of the Bind set to 87 (i.e., RU size = 1024 bytes).

Bytes 10 and 11 in the BIND can contain the following values (in hexadecimal):

BIND Value	Maximum RU Size
85	256
95	288
A5	320
B5	352
C5	384
D5	416
E5	448
F5	480
86	512
96	576
A6	640
B6	704
C6	768
D6	832
E6	896
F6	960
87	1024

7.5.4.4.1 Chaining Considerations when Using Small RU Sizes

Only one HSM command can be sent outbound per chain, and if a command is sent to the HSM in multiple RUs, the RUs must be chained. Chain elements are concatenated in the HSM and the data is not given to the command processor until the LIC element is received.
The internal buffer is limited to 1024 HSM bytes, so no command, regardless of the number of RUs in the chain, can exceed 1023 bytes total. If a command produces a response containing more data than the inbound or SLU "maximum RU size" specified in the Bind, the HSM blocks the reply into multiple RUs. All response RUs resulting from one HSM command are chained together by the HSM.

7.5.4.4.2 Performance Considerations when Using Small RU Sizes

From HSM Functional Revision 5.03, data is buffered and passed to the SNA communications output buffer in appropriate-size blocks after the HSM command has been completed. Therefore some degradation in system performance occurs (compared with earlier Functional Revisions) when the RU sizes selected in the Bind are less than 1024 bytes. Select the maximum RU size supported in the Host system to reduce the tendency to subdivide long messages in the HSM. This helps to maximise the Host/HSM system transaction throughput.

To maintain system performance, when the RU size is set to 1024 bytes, program the HSM to disable the double buffering required for small RU sizes. When the double buffering is disabled, data is stored directly into the communications output buffer, thus eliminating any performance degradation.

7.5.4.5 Multiple Reply Requests

Most Host commands produce only one reply request; this request carries OIC (BC & EC bits set) and CD set. However, the HSM printing commands (i.e., PE, OA, OE and OG) produce two reply requests and the PIN solicitation processing command can produce as many as 52. The HSM chains these multiple replies together with the last in chain (BC not set & EC set) carrying CD.

7.5.4.6 SHUTD

If data traffic is disabled using SHUTD, any FMD requests sent outbound after the HSM has returned SHUTC are ignored. The appropriate session-level responses are returned, but data is discarded.

7.5.4.7 Character-Coded Logons

The HSM has no provision for supplying character-coded logons; the Host application or VTAM is responsible for starting the LU-LU session.

7.5.4.8 SSCP-LU Session

The HSM ignores FMD requests on the SSCP-LU session; a positive response is returned, but data is discarded.

7.5.4.9 Transparent Mode

Normally, the HSM searches for and discards embedded orders in the 3270 data stream in outbound requests. However, to maximise throughput and allow binary data, the HSM has a "transparent" mode. No order stripping is done in transparent mode, and the Host application must ensure that no 3270 orders are sent. The HSM includes the read header in all inbound FMD requests regardless of mode.

7.5.5 Host NCP Configuration

Details of a typical NCP configuration for use with the SNA HSM are shown in Appendix D.

7.6 TCP/IP Protocol

The HSM employs TCP for the transfer of data (see Chapter 1). It acts as a TCP server supporting multiple TCP clients configurable via the CH command. The maximum number of TCP connections that can be supported is 8. If a TCP client attempts to establish a connection with an HSM that already has the maximum number of configured connections active, the TCP client's request is rejected.

The HSM supports the TCP Push function. To improve the efficiency of data transfer the TCP protocol software can buffer data into larger blocks, or divide the data into smaller blocks. This is useful for time-critical applications, such as transaction processing systems, where response time is more important than Ethernet utilisation efficiency.

The HSM always returns a response to a command using the Push function.

7.6.1 Sending Commands

The HSM expects a command to be sent in the form defined in the table.

Field	Size	Format	Description
LENGTH	2	Byte	Length of the COMMAND field
COMMAND	n	Byte	HSM command
Note: The field COMMAND should not be bracketed by X'02 - X'03 as used with the Async protocol.			

Multiple commands can be sent to an HSM within one TCP transmission. Each should be of the form defined in the table.

Example:

The command format for a diagnostics command (NC) is:

X'00 X'06 X'31 X'32 X'33 X'34 X'4E X'43

where the HSM message header length is set to 04, a message header of 1234 is used, and character representation is ASCII.

7.6.2 Returning Responses

When the HSM receives a command from a TCP client, the command is processed and the response returned to the TCP client. The response is of the form defined in the table.

Field	Size	Format	Description
LENGTH	2	Byte	Length of the RESPONSE field
RESPONSE	n	Byte	HSM response
Note: The field RESPONSE is not bracketed by X'02 - X'03 (or alternative value) as used with the Async protocol.			

The result of each command sent to an HSM is returned as a separate response to the TCP client. This also operates when multiple commands are sent to the HSM in a single TCP transmission.
All HSM responses are returned to the TCP client using the TCP Push function.

Example:

The response format from a diagnostics command (NC) is:

X'00	X'18	X'31	X'32	X'33	X'34	X'4E	X'43	X'30	X'30	X'32	X'36
X'38	X'36	X'30	X'34	X'37	X'34	X'34	X'34	X'39	X'31	X'32	X'34
X'32	X'32	X'30	X'30	X'30	X'37	X'2D	X'45	X'30	X'30	X'30	

where the HSM message header length is set to 04, a message header of 1234 is used, and the character representation is ASCII.

The example shows the error code returned was 00 and the LMK check value returned was 2686047444912422 and the firmware installed is 0007-E000.

7.7 UDP Protocol

The HSM client expects all UDP connections to be made on the Well-Known-Port at the IP address (see Chapter 1). The IP address and Well-Known-Port address are defined to the HSM when configuring the software settings with the Console CH command.

All UDP host clients sending data to the HSM send the datagrams to the Well-Known-Port at the IP address. The HSM (UDP server) processes the datagram and returns a datagram response to the originating UDP host client.

UDP is a connection-less protocol. If the HSM detects an error in a received datagram it is discarded. The UDP host client should support a time-out mechanism whereby if a response is not received within the time-out period the original request is re-sent.

7.7.1 Sending Commands

The HSM expects a command to be sent in the form defined in the table.

Field	Size	Format	Description
LENGTH	2	Byte	Length of the COMMAND field
COMMAND	n	Byte	HSM command
Note: The field COMMAND should not bracketed by X'02 - X'03 as used with the Async protocol.			

Only a single command can be sent to an HSM in one UDP transmission (packet).

Example:
The command format for a diagnostics command (NC) is:

X'00 X'06 X'31 X'32 X'33 X'34 X'4E X'43

where the HSM message header length is set to 04, a message header of 1234 is used, and character representation is ASCII.

7.7.2 Returning Responses

When the HSM receives a command from a UDP client the command is processed and the response returned to the UDP client. The response is of the form defined in the table.

Field	Size	Format	Description
LENGTH	2	Byte	Length of the RESPONSE field
RESPONSE	n	Byte	HSM response
Note: The field RESPONSE is not bracketed by X'02 - X'03 (or alternative value) as used with the Async protocol.			

The result of each command sent to an HSM is returned as a separate response to the UDP client.

Example:
The response format from a diagnostics command (NC) is:

X'00	X'18	X'31	X'32	X'33	X'34	X'4E	X'43	X'30	X'30	X'32	X'36
X'38	X'36	X'30	X'34	X'37	X'34	X'34	X'34	X'39	X'31	X'32	X'34
X'32	X'32	X'30	X'30	X'30	X'37	X'2D	X'45	X'30	X'30	X'30	

where the HSM message header length in set to 04, a message header of 1234 is used, and the character representation is ASCII.

The example shows the error code returned was 00 and the LMK check value returned was 2686047444912422 and the firmware installed is 0007-E000.

CHAPTER 4

LOCAL MASTER KEYS

CONTENTS

Page

1 GENERAL 4-1

2 GENERATING THE LMK COMPONENTS 4-3
2.1 GENERATING COMPONENT SET 1 4-4
2.2 GENERATING COMPONENT SET 2 4-6
2.3 GENERATING COMPONENT SET 3 (ETC.) 4-6
2.4 PASSWORD MODE 4-6

3 LOADING THE LMKS 4-7

4 MOVING 'OLD' LMKS INTO KEY CHANGE STORAGE 4-10

5 TRANSLATING ENCRYPTED DATA 4-11

6 VERIFYING THE CONTENTS OF THE LMK STORE 4-11

7 DUPLICATING LMK COMPONENT SETS 4-12

8 LOADING THE TEST KEYS 4-13

1 GENERAL

The HSM Local Master Keys (LMKs) are numbered from key 00 to key 99. They are used in pairs and each pair has a function, as shown in the table.

LMK Pair	Function
00 - 01	Contains the two Smart Card “keys” (Passwords if the HSM is configured for Password mode) required for setting the HSM into the Authorized state.
02 - 03	Encrypts the PINs for Host storage.
04 - 05	Encrypts Zone Master Keys and double-length ZMKs.
	Encrypts Zone Master Key components under a Variant.
06 - 07	Encrypts the Zone PIN keys for interchange transactions.
08 - 09	Used for random number generation.
10 - 11	Used for encrypting keys in HSM buffer areas.
12 - 13	The initial set of Secret Values created by the user; used for generating all other Master Key pairs.
14 - 15	Encrypts Terminal Master Keys, Terminal PIN Keys, and PIN Verification Keys.
	Encrypts Card Verification Keys under a Variant.
16 - 17	Encrypts Terminal Authentication Keys.
18 - 19	Encrypts reference numbers for solicitation mailers.
20 - 21	Encrypts ‘not on us’ PIN Verification Keys and Card Verification Keys under a Variant.
22 - 23	Encrypts Watchword Keys.
24 - 25	Encrypts Zone Transport Keys.
26 - 27	Encrypts Zone Authentication Keys.
28 - 29	Encrypts Terminal Derivation Keys.
30 - 31	Encrypts Zone Encryption Keys.
32 - 33	Encrypts Terminal Encryption Keys.
34 - 35	Encrypts RSA Keys.
36 - 99	Reserved for future use.
There are Variants of some keys to suit particular requirements.	

The Local Master Keys are normally generated once, recorded on Smart Cards and loaded into the HSM. If the HSM is opened for any reason (e.g. maintenance), the keys are erased and therefore must be reloaded.

To generate and load the LMKs, at least three "Component Holders" (two Authorising Officers and at least one other person) are required.

The first Authorising Officer creates two 16-digit Secret Values (and a Password, if the HSM is configured in Password mode), and enters this data at the Console. The two Secret Values are temporarily stored internally as key pair 12 - 13. The HSM generates new values for the other keys shown in the table. The new values are called a "Component Set". This set of values is then recorded on a Smart Card.

Using the same procedure, the second Authorising Officer creates two Secret Values (and if necessary, a password), generates a Component Set and records it on a second Smart Card.

The third Component Holder creates two Secret Values, generates a Component Set and records it on a third Smart Card.

More than three people can be involved.

The procedure results in a number of Smart Cards, each containing one Component Set of keys. The first and second Smart Cards also contain Authorising data. Each Component Holder makes copies of its data so that it is stored on a number of Smart Cards. At least two copies should be made, one for storage onsite and one offsite. Serious consideration should be given to the creation of extra copies to provide a greater level of resilience against the failure of any one Smart Card.

NOTE: AT NO TIME SHOULD ANY ONE PERSON BE ABLE TO GAIN ACCESS TO ALL COMPONENTS.

The data contained in the Smart Cards is loaded to LMK storage. The load function stores Authorising data (Passwords, if this mode is used) as key pair 00 - 01, and mathematically combines each Component Set with the previous contents of the LMK storage to form the remaining LMK pairs. The Smart Cards must then be separately and securely stored (e.g., in safe deposit boxes).

When new LMKs are generated (for example, if existing keys are known to be compromised), it is usually necessary to save the old LMKs so that existing encrypted data can be translated from encryption under the old keys to encryption under the new keys. To save the LMKs, transfer them to a special memory area known as "key change storage". After this process, use Host commands to translate the old encrypted data.

The LMKs in the unit can be verified and the LMKs on the Smart Cards (or PROMs) can be checked. It is recommended that:

- LMKs in the HSM are verified at 6-month intervals.
- LMKs on Smart Cards (including all the spare copies) are checked at 12-month intervals.
- LMKs are changed at 2 year intervals. This ensures that the procedures required for the change are regularly exercised and updated where necessary.

2 GENERATING THE LMK COMPONENTS

The following are required:

- The three (or more) Component Holders (two Authorising Officers plus at least one other Component Holder), who are to generate the three (or more) sets of components. (The two Authorising Officers must be present whenever the HSM is to be set into the Authorised state).
- The HSM Console.
- Access to a single HSM.
- At least 6 formatted blank Smart Cards (up to 12 can be used). 6 cards provide two copies of three sets of components, 12 cards provide four copies of three sets. (Note that new cards are supplied un-formatted. Use the FC command to format or re-format the cards).
- Labels for identifying the Smart Cards.
- A log to record the LMK check values that are used to verify the contents of each Smart Card at a later date. (If the HSM is configured in Password mode and the two Passwords are entered by the Authorising Officers (i.e., not automatically created by the HSM and stored electronically), the two Passwords must be also recorded in the log).
- The two keys for the cam locks, and the key for the KEY switch.

The results of the process with three Component Holders and two copies of the Smart Cards are three Smart Card sets as follows:

- Smart Card set 1, consisting of one original Smart Card plus one duplicate (contains Component Set 1 (and, if applicable, Password 1)).
- Smart Card set 2, consisting of one original Smart Card plus one duplicate (contains Component Set 2 (and, if applicable, Password 2)).
- Smart Card set 3, consisting of one original Smart Card plus one duplicate (contains Component Set 3).

The Secret Values must each be 16 random characters, and can contain any hexadecimal characters (0-9, A-F).

Note that during the process of creating an LMK component set a number of values (Secret Values A and B and Value C) can be either entered manually or randomly generated by the HSM, and if the values are entered manually and written down for storage, it is possible to subsequently re-create the LMK components even if the Smart Cards are not available. Therefore the recorded values must be MORE SECURELY STORED than the Smart Cards.

2.1 Generating Component Set 1

In the description that follows, user entries at the Console are shown underlined. Characters returned by the HSM that depend on the values entered by the user (and therefore cannot be predicted) are shown as X.

It is assumed that the HSM has been set for Smart Card mode and Echo On at configuration (Chapter 3, CS command).

(1) Set the HSM offline: insert the key in the KEY switch on the HSM rear panel and rotate it clockwise one quarter turn, then allow it to spring back. The Console displays:

HSM going OFFLINE, press Reset to go Online.
Master Key loading facilities now available.
Offline >

(2) Initiate the LMK generation and storage procedure. Use the GK command. The HSM responds with a series of prompts to ensure that the initial starting conditions are achieved.

Offline > GK <Return>

The HSM responds with:
WARNING - Physical keys required; proceed? [Y/N]: Y <Return>

(3) In response to prompts from the HSM:

- Pull the arming ring on the HSM rear panel
- Gain access to the inside of the HSM (described in Chapter 2).

WARNING: SEE THE WARNINGS IN APPENDIX F.

- Behind the front cover of the HSM is a box, 152mm x 140mm (6 in x 5.5 in) which contains the tamper-detection switches. The switch to the left of the box is the tamper-detection arming switch. Set the switch to the left.

(4) The HSM prompts for the number of the component set:
LMK component set [1-9]: 1 <Return>

(5) The HSM prompts for the first (16-character hexadecimal) secret value:

Enter secret value A: a a a a a a a a a a a a a a a a <Return>

(If Echo off has been configured, the characters are replaced by stars *)
If only <Return> is entered, the HSM generates a random number for use as the secret value.

(6) The HSM prompts for the second (16 character hexadecimal) secret value:

Enter secret value B: a a a a a a a a a a a a a a a a <Return>

As in Step 5, just <Return> can be entered.

(7) The HSM prompts for the third (8- character decimal) value, which may (for example) be the date:

Enter value C: 18051994 <Return>

As in Step 5, just <Return> can be entered.

(8) The HSM is now ready to copy the LMKs onto Smart Cards. It prompts:

Insert blank card and enter PIN: ***** <Return>

Insert the Smart Card in the reader and enter its PIN.

If there is a fault on the card or it already has data on it, either allow the HSM to write over the old data or reject the card and use another, as applicable, in reply to prompts from the HSM.

(9) The HSM displays:

Device write complete, check: XXXX XXXX XXXX XXXX

Remove the Smart Card and store it securely. If a failure has occurred, the Smart Card is ejected: return to Step 8.

Make a note of the check value for future reference. (It is subsequently used to ensure that the contents of the Smart Card are correct, and should be safely stored.)

The HSM prompts:

Make another copy? [Y/N]: Y <Return>

(10) Make another copy: repeat Steps 9 and 10 until the required number of copies have been made, then terminate the command in response to the prompt:

Make another copy? [Y/N]: N <Return>

X copies made

2.2 Generating Component Set 2

The procedure of generating Component Set 2 is almost the same as the procedure for generating Component Set 1.

(1) In Step (4), enter 2 (for Component Set 2) instead of 1.

2.3 Generating Component Set 3 (etc.)

The procedure for generating Component Set 3 (and 4 to 9, as required) is almost the same as the procedure for generating Component Set 1.

(1) In Step (4) enter 3 (or 4, etc.) instead of 1.

(2) When all component sets have been generated, to return the HSM to normal use, load the LMKs, close the unit, slide it into its cabinet, lock the cam locks, remove all three keys. Press the RESET button on the rear panel and pull the tamper-detection ring. Confirm that the ARMED indicator on the front panel is illuminated.

2.4 Password Mode

To configure the HSM in Password mode, see Generating Component Sets 1, 2 and 3.

In Step (5) the HSM prompts twice for the (16- character alphanumeric) Password before prompting for the secret values.

3 LOADING THE LMKS

The HSM Master Keys are loaded when a HSM is first put into service. Also, because keys are erased whenever the HSM is opened, they must subsequently be reloaded. The procedure for loading from Smart Cards is described, with reference to loading from PROMs for compatibility with RG6000 HSM systems.

The following are required:

- One Smart Card from each of the Sets, or one PROM from each of the three PROM sets, as applicable.
- The Component Holders responsible for Smart Card (or PROM) custody. (No one person should have access to all Smart Cards or PROMs).

In the description that follows, user entries at the Console are shown underlined. Characters returned by the HSM that depend on the values entered by the user (and therefore cannot be predicted) are shown as X.

The order in which the Smart Cards (or PROMs) are loaded into the HSM is not important, but, for convenience, they are referred to as the first, second and third (etc.) Smart Cards (or PROMs).

Before handling PROMs, touch a grounded object (such as the HSM) to discharge any static electricity.

(1) Set the HSM offline: insert the key in the KEY switch on the HSM rear panel and rotate it clockwise one quarter turn, then allow it to spring back. The Console displays:

HSM going OFFLINE, press Reset to go Online.

Master Key loading facilities now available.

Offline >

(2) Initiate the LMK loading. Use the LK command. The HSM responds with a series of prompts to ensure that the initial starting conditions are achieved.

Offline > LK <Return>

The HSM responds with:

WARNING - Physical keys required; proceed? [Y/N]: Y <Return>

(3) In response to prompts from the HSM:

- Pull the arming ring on the HSM rear panel.
- Gain access to the inside of the HSM (described in Chapter 2).

WARNING: SEE THE WARNINGS IN APPENDIX F

- Behind the front cover of the HSM is a box, 152mm x 140mm (6 in x 5.5 in) which contains the tamper-detection switches. The switch to the left of the box is the tamper-detection arming switch. Set the switch to the left.

(4) The HSM prompts for the components:

Load LMK from components.

Insert device and press ENTER: <Return>

Insert the first Smart Card or fit the first PROM, as applicable.

In the case of a Smart Card, insert it into the card reader on the front of the panel of the HSM.

In the case of a PROM, fit it into the Zero Insertion Force (ZIF) socket located at the front left of the circuit board. The ZIF socket has a small lever arm which can be raised and lowered. Ensure that the ZIF socket is in the open position before inserting the PROM. The PROM must be handled carefully. At one end of the device there is a small notch; place the PROM in the ZIF socket with the notch towards the centre of the board. Move the lever arm on the ZIF socket to hold the PROM securely.

(5) When the device is inserted/fitted, press:

<Return>

(6) In the case of a Smart Card, the HSM prompts:

Enter PIN: * * * * * <Return>

Enter the PIN.

(7) The HSM reads the Smart Card (or PROM) then displays:

CHECK = XXXX XXXX XXXX XXXX

Load further components? [Y/N]: Y <Return>

If it displays an error message, rectify the fault and repeat the operation as necessary.

When successful, remove the Smart Card (or PROM).

(8) Insert the second Smart Card (or PROM) and repeat the loading procedure, Steps 4 to 7.

(9) Repeat Step 8 for the third (and any subsequent) set of components. When all have been loaded and the HSM displays the check value, RECORD THE CHECK VALUE (it is the check on the final LMK pairs and is subsequently used to verify that the LMK pairs are correct), then press N to terminate the loading procedure:

CHECK = XXXX XXXX XXXX XXXX

Load further components? [Y/N]: N <Return>

(10) It is now possible to go to the key change storage procedure (Step 4), if required. Otherwise close the HSM, slide it into its cabinet, lock the cam locks, remove all three keys.

(11) Ensure that the HSM can be set into the Authorized state by inserting the Smart Cards or entering the Passwords (as applicable). Use the A command, and insert the Smart Cards and enter the PINs (or enter the Passwords), in response to prompts. If used, the Passwords must be entered in the correct order (i.e., the first should be the Password loaded with Component Set 1).

Online > A < Return >

Enter the first PIN (or the Password), as applicable:

First Officer:

Insert card and enter PIN: * * * * * < Return >

or

Password: * * * * * * * * * * * * * * * * < Return >

Enter the second PIN (or the Password), as applicable:

Second Officer:

Insert card and enter PIN: * * * * * < Return >

or

Password: * * * * * * * * * * * * * * * * < Return >

When successful the HSM displays:

AUTHORIZED

Online - AUTH >

If one of the PINs (or Passwords) does not have the correct number of characters (excluding spaces), the HSM re-prompts, and, if one was incorrect it returns NOT AUTHORIZED. In either case, press <Delete> and re-enter the PINs (or Passwords).

(12) Press the RESET button on the rear panel to set the HSM online to the Host. This also removes the HSM from the Authorised state.

(13) Pull the tamper-detection arming ring at the HSM rear panel. All Component Holders responsible for security should confirm that this has been done, and that the ARMED indicator on the front panel is illuminated.

4 MOVING 'OLD' LMKS INTO KEY CHANGE STORAGE

When new LMKs have been loaded into the HSM, using the LK command, the HSM prompts whether a set of old LMKs needs to be loaded into Key Change Storage for use in translations from old to new keys. If so, proceed as follows:

(1) Enter Authorised state:

Offline > A <Return>

First Officer

Insert card and enter PIN: **** <Return>

Second Officer

Insert card and enter PIN: **** <Return>

AUTHORISED

Offline - Auth >

(2) Initiate moving 'Old' keys into key change storage. Use the LO command:

Offline - Auth > LO < Return >

Load Old LMK from components.

Insert device, press ENTER when ready: < Return >

Insert the first (old) Smart Card or PROM as applicable.

(3) When the device is inserted/fitted, press:

< Return >

(4) In the case of a Smart Card, the HSM prompts:

Enter PIN: ***** < Return >

Enter the PIN.

(5) The HSM reads the Smart Card (or PROM) then displays:

CHECK = XXXX XXXX XXXX XXXX

Load further components? [Y/N]: Y <Return>

If it displays an error message, rectify the fault and repeat the operation as necessary.

When successful, remove the Smart Card (or PROM).

(6) Insert the second Smart Card (or PROM) and repeat the procedure from Steps 2 to 4.

(7) Repeat Step 5 as necessary until all old component sets have been moved into key change storage. When all have been moved and the HSM displays the check value, press N to terminate the procedure:

CHECK = XXXX XXXX XXXX XXXX

Load further components? [Y/N]: N <Return>

(8) Return the HSM to normal use, as described in Generating Component Set 3, Step (2).

5 TRANSLATING ENCRYPTED DATA

When the HSM is ready to translate data from encryption under the old LMKs to encryption under the new LMKs, (i.e., it has the new keys loaded and the old keys in key change storage), it requires the Host to send the correct sequence of commands for each encrypted set of data that needs translating (see the Programmer's Manual).

On completion, ensure that all the HSMs fitted with the old LMKs are updated and that all the units are closed, locked, and reset, and their tamper-detection circuits are armed.

6 VERIFYING THE CONTENTS OF THE LMK STORE

The LMKs installed in the HSM should be checked periodically. Using the V command, confirm that the check value is identical to the value that was recorded when the LMK set was installed.

Online > V < Return >

The HSM responds with:

Master Key check: XXXX XXXX XXXX XXXX

Confirm that the check value is the same as the one logged when the LMKs were first loaded. If the contents of LMK storage in the HSM have been corrupted, the HSM responds with:

MASTER KEY CHECK = MASTER KEY PARITY ERROR

(LMK storage can also be verified by a Host command).

The original and duplicate LMK Smart Cards should be checked periodically. Refer to the VC Command in Chapter 5.

7 DUPLICATING LMK COMPONENT SETS

The LMK component set on a Smart Card can be copied onto another Smart Card using the DC command.

(1) The HSM must be offline (see Generating Component Set 1, Step 1).

(2) Initiate the copying procedure:

Offline > DC < Return >

Press Y in response to the HSM prompt:

WARNING - Physical keys and LMK components required; proceed ? [Y/N]: Y
< Return >

(3) The HSM must be armed, opened, and the bypass switch set.

(4) The HSM prompts:

Insert card to be duplicated and enter PIN: * * * * * <Return>

CHECK = XXXX XXXX XXXX XXXX

Insert the original card, enter its PIN and confirm the check value.

(5) The HSM prompts:

Insert blank card and enter PIN: * * * * * <Return>

Insert a new formatted card and enter its PIN.

If the HSM displays:

WARNING CARD CONTAINS LMK SET, OVERWRITE? [Y/N]:

Either press Y <Return> if the old data is to be overwritten (for example, an old Smart Card being reused), or, if necessary (for example if the wrong Smart Card has been inserted), press N <Return> to terminate the command.

(6) When the Smart Card has been successfully overwritten, the HSM displays:

Device write complete, check: XXXX XXXX XXXX XXXX

Remove device and store securely

Make another copy? [Y/N]:

Confirm the check value.

If another copy is required press Y <Return> and repeat Steps 4 to 6. Otherwise return the HSM to normal use as described in Generating Component Set 3, Step 2.

8 LOADING THE TEST KEYS

It is good security practice to ensure that the LMK pairs used in the operational system are not used during test operations. It is useful to have a set of known Test LMKs to simplify cryptographic fault-finding. It also helps the manufacturer to diagnose cryptographic problems if they know the LMK pairs. Therefore, all customers are provided with an identical "Test Key Smart Card". To load this device, use the LK command, with the Smart Card in the reader in the normal way.

The values of the LMK pairs contained in the Test Key Smart Card are shown in Figure 4.1. The two Passwords are also held in this device, and their values are shown in Figure 4.1.

The PIN for the Test Key Smart Card is:

1 2 3 4

LMK	Contents								LMK	Contents							
00	01	01	01	01	01	01	01	01	01	79	02	CD	1F	3	6E	F8	BA
02	20	20	20	20	20	20	20	20	03	31	31	31	31	31	31	31	31
04	40	40	40	40	40	40	40	40	05	51	51	51	51	51	51	51	51
06	61	61	61	61	61	61	61	61	07	70	70	70	70	70	70	70	70
08	80	80	80	80	80	80	80	80	09	91	91	91	91	91	91	91	91
10	A1	A1	A1	A1	A1	A1	A1	A1	11	B0	B0	B0	B0	B0	B0	B0	B0
12	C1	C1	01	01	01	01	01	01	13	D0	D0	01	01	01	01	01	01
14	E0	E0	01	01	01	01	01	01	15	F1	F1	01	01	01	01	01	01
16	1C	58	7F	1C	13	92	4F	EF	17	01	01	01	01	01	01	01	01
18	01	01	01	01	01	01	01	01	19	01	01	01	01	01	01	01	01
20	02	02	02	02	02	02	02	02	21	04	04	04	04	04	04	04	04
22	07	07	07	07	07	07	07	07	23	10	10	10	10	10	10	10	10
24	13	13	13	13	13	13	13	13	25	15	15	15	15	15	15	15	15
26	16	16	16	16	16	16	16	16	27	19	19	19	19	19	19	19	19
28	1A	1A	1A	1A	1A	1A	1A	1A	29	1C	1C	1C	1C	1C	1C	1C	1C
30	23	23	23	23	23	23	23	23	31	25	25	25	25	25	25	25	25
32	26	26	26	26	26	26	26	26	33	29	29	29	29	29	29	29	29
34	2A	2A	2A	2A	2A	2A	2A	2A	35	2C	2C	2C	2C	2C	2C	2C	2C
36	2F	2F	2F	2F	2F	2F	2F	2F	37	31	31	31	31	31	31	31	31
38	01	01	01	01	01	01	01	01	39	01	01	01	01	01	01	01	01

Password 1 = 01 01 01 01 01 01 01 01

Password 2 = NOW IS THE TIME FOR A

Figure 4.1 – LMK Pairs (and Passwords) on the Test Key Smart Card

The check value is 2686 0474 4491 2422

CHAPTER 5

OPERATING INSTRUCTIONS

CONTENTS

		Page
1	LIST OF CONSOLE COMMANDS	5-1
2	GENERAL	5-3
3	THE AUTHORISED STATE	5-4
3.1	ENTERING THE AUTHORISED STATE	5-4
3.2	CANCELLING THE AUTHORISED STATE	5-5
4	VIEWING HSM STATUS INFORMATION	5-6
4.1	VIEWING HSM AUXILIARY PORT CONFIGURATION INFORMATION	5-6
4.2	VIEWING HSM CONSOLE PORT CONFIGURATION INFORMATION	5-6
4.3	VIEWING HSM HOST PORT CONFIGURATION INFORMATION	5-7
4.4	VIEWING THE HSM SOFTWARE REVISION NUMBER	5-9
5	KEY MANAGEMENT FUNCTIONS	5-10
5.1	KEY TYPE TABLE	5-10
5.2	KEY SCHEME TABLE	5-11
5.3	GENERATE KEY COMPONENT	5-11
5.4	GENERATE KEY COMPONENTS AND WRITE TO SMART CARD	5-12
5.5	ENCRYPT CLEAR COMPONENT	5-13
5.6	FORM KEY FROM COMPONENTS	5-14
5.7	GENERATE KEY	5-16
5.8	IMPORT KEY	5-18
5.9	EXPORT KEY	5-19
6	ZONE MASTER KEY FUNCTIONS	5-20
6.1	GENERATING A ZONE MASTER KEY COMPONENT	5-20
6.2	GENERATE A ZONE MASTER KEY, WRITE COMPONENTS TO SMARTCARDS	5-21
6.3	ENCRYPTING A CLEAR ZONE MASTER KEY COMPONENT	5-22
6.4	FORMING A ZONE MASTER KEY FROM ENCRYPTED COMPONENTS	5-23
6.5	IMPORTING A CVK OR PVK FROM ZMK TO LMK	5-24
7	ZONE PIN KEY FUNCTIONS	5-25
7.1	GENERATING A ZONE PIN KEY (VISA ACQUIRER OR ISSUER WORKING KEY)	5-25
7.2	TRANSLATING A ZONE PIN KEY	5-26
8	TERMINAL KEY FUNCTIONS	5-27
8.1	ENCRYPTING A KEY UNDER LMK PAIR 14-15	5-27
9	KEY COMPONENT FUNCTIONS	5-28
9.1	FORM A KEY FROM COMPONENTS	5-28
10	GENERATING A CHECK VALUE	5-30
11	CARD VERIFICATION KEY MANAGEMENT	5-32
11.1	GENERATING A CVK PAIR	5-32

Zaxus

11.2 TRANSLATING A CVK PAIR FROM ENCRYPTION UNDER THE LMK TO ENCRYPTION UNDER A ZMK 5-33

12 VISA VERIFICATION FUNCTIONS 5-34
12.1 GENERATING A VISA CARD VERIFICATION VALUE 5-34
12.2 GENERATING A VISA PIN VERIFICATION VALUE 5-35

13 LOADING THE DIEBOLD TABLE 5-36

14 DUKPT CONSOLE COMMANDS 5-38
14.1 GENERATE A DOUBLE-LENGTH *ZMK COMPONENT 5-38
14.2 FORM A *ZMK FROM CLEAR COMPONENTS 5-39
14.3 IMPORT A BASE DERIVATION KEY (*BDK) 5-40
14.4 GENERATE A BASE DERIVATION KEY (*BDK) 5-41

15 DIAGNOSTIC TEST 5-42

16 DES CALCULATOR 5-43
16.1 SINGLE-LENGTH KEY CALCULATOR 5-43
16.2 DOUBLE-LENGTH KEY CALCULATOR 5-44

17 SMART CARDS 5-45
17.1 FORMATTING A SMART CARD 5-45
17.2 CREATING AN AUTHORISING OFFICER SMART CARD 5-46
17.3 VERIFYING THE CONTENTS OF A SMART CARD 5-47
17.4 CHANGING A SMART CARD PIN 5-47
17.5 READING UNIDENTIFIABLE SMART CARD DETAILS 5-48
17.6 COPYING A PROM TO A SMART CARD 5-49

18 VISA CASH SYSTEM 5-50
18.1 GENERATE AND EXPORT A MASTER LOAD KEY (*KML) 5-50
18.2 IMPORTING A MASTER LOAD KEY (*KML) 5-51

19 AMERICAN EXPRESS CARD SECURING CODE 5-52
19.1 GENERATE A CSCK 5-52
19.2 EXPORT A CSCK 5-53
19.3 IMPORT A CSCK 5-54

1 LIST OF CONSOLE COMMANDS

Console Command	Function	Chapter	Page
A	Entering the Authorised State	5 - 3.1	4
B	Generating a Zone PIN Key (VISA Acquirer or Issuer Working Key)	5 - 7.1	25
BK	Form a Key from Components	5 - 9.1	28
C	Cancelling the Authorised State	5 - 3.2	5
CA	Configure the HSM Auxiliary port.	3 - 5	3 - 8
CC	Configure the HSM Console port.	3 - 3	3 - 5
CH	Configure the HSM Host port.	3 - 6	3 - 9
	Async	3 - 6.1	3 -
	Bisync	3 - 6.2	3 -
	SDLC	3 - 6.4	3 -
	SNA-SDLC	3 - 6.5	3 -
	Ethernet	3 - 6.6	3 -
CK	Generating A Check Value	5 - 10	30
CO	Creating an Authorising Officer Smart Card	5 - 17.2	46
CS	Configure Security. Set the HSM security configuration and some processing parameters.	3 - 4	3 - 6
CV	Generating a VISA Card Verification Value	5 - 12.1	34
D	Forming a Zone Master Key From Encrypted Components	5 - 6.4	23
DA	Generate and Export a Master Load Key (*KML)	5 - 18.1	50
DB	Importing a Master Load Key (*KML)	5 - 18.2	51
DC	Copy the LMK Component Set from one Smart Card to another.	4 - 7	4 - 13
DD	Generate a Double-Length *ZMK Component	5 - 14.1	38
DE	Form a *ZMK from Clear Components	5 - 14.2	39
DF	Import a Base Derivation Key (*BDK)	5 - 14.3	40
DG	Generate a Base Derivation Key (*BDK)	5 - 14.4	41
DT	Diagnostic Test	5 - 15	42
EC	Encrypt Clear Component	5 - 5.5	13
F	Generating a Zone Master Key Component	5 - 6.1	20
FC	Formatting a Smart Card	5 - 17.1	45
FK	Form Key from Components	5 - 5.6	14
GC	Generate Key Component	5 - 5.3	11
GK	Generate (and store) an LMK Component Set.	4 - 2.1	4 - 4

Console Command	Function	Chapter	Page
GS	Generate Key Components and write to Smart Card	5 - 5.4	12
GZ	Generate a Zone Master key, Write Components to Smartcards	5 - 6.2	21
IV	Importing a CVK or PVK from ZMK to LMK	5 - 6.5	24
K	Encrypting a Key Under LMK Pair 14-15	5 - 8.1	50
KA	Generating a CVK Pair	5 - 11.1	32
KB	Translating a CVK Pair from Encryption Under the LMK to Encryption Under a ZMK	5 - 11.2	33
KE	Export Key	5 - 5.9	19
KG	Generate Key	5 - 5.7	16
KI	Import Key	5 - 5.8	18
LK	Load HSM master keys (LMKs).	4 - 3	4 - 7
LO	Move 'old' LMKs into Key Change Storage, for use in subsequent translations.	4 - 4	4 - 10
N	Single-Length Key Calculator	5 - 16.1	43
NP	Changing a Smart Card PIN	5 - 17.4	47
PC	Copying a PROM to a Smart Card	5 - 17.6	49
PV	Generating a VISA Pin Verification Value	5 - 12.2	35
QA	Viewing HSM Auxiliary Port Configuration Information	5 - 4.1	6
QC	Viewing HSM Console Port Configuration Information	5 - 4.2	6
QS	Query Security. Display the HSM security configuration and other parameters set by the CS command.	3 - 4	3 - 6
QH	Viewing HSM Host Port Configuration Information	5 - 4.3	7
R	Loading the Diebold Table	5 - 13	36
RC	Reading Unidentifiable Smart Card Details	5 - 17.5	48
V	Verify the LMK contents	4 - 6	4 - 11
VC	Verifying the Contents of a Smart Card	5 - 17.3	47
VR	Viewing the HSM Software Revision Number	5 - 4.4	9
WK	Translating a Zone PIN Key	5 - 7.2	26
YA	Generate a CSCK	5 - 19.1	52
YB	Export a CSCK	5 - 19.2	53
YC	Import a CSCK	5 - 19.3	54
Z	Encrypting a Clear Zone Master Key Component	5 - 6.3	22
$	Double-Length Key Calculator	5 - 16.2	44

2 GENERAL

The HSM is normally online to the Host and does not require operator monitoring or intervention. In use the HSM performs cryptographic processing in response to commands from the Host. Some commands are actioned by the user at the HSM Console terminal. These include commands involving plain text data, system configuration and others that do not concern the Host.

This chapter details the commands that can be entered at the Console with the exception of the commands associated with equipment installation and LMK management, which are described in Chapters 4 and 5 as applicable.

Entry of commands and data at the Console is not case sensitive (i.e., A has the same effect as a). Spaces can be inserted between characters to ease legibility during entry; they are ignored by the HSM. However they cannot be used between command characters (e.g. the LK command can not be successfully entered as L K).

When entering sensitive (clear text) data, use the Inhibit Echo Back facility to ensure that the HSM does not echo the data to the Console screen. This is set at configuration (Chapter 3). Instead of displaying the data, the HSM displays a star for each character entered. Thus:

0123456789ABCDEF

is shown on the screen as:

* * * * * * * * * * * * * * * *

To exit from a command during data entry, press the <Delete> key (or <Control> and C simultaneously). The HSM responds with:

TERMINATED

3 THE AUTHORISED STATE

The Authorised state is required for functions involving clear text data.

3.1 Entering the Authorised State

Command:	A (Can be used online and offline).
Function:	To set the HSM into the Authorised state.
	The HSM prompts for either Smart Card entry or Passwords, as applicable.
Inputs:	PIN: 4 to 8 alphanumeric characters.
	Password (if applicable): 16 alphanumeric characters.
Outputs:	Text messages as shown in examples.
Errors:	Reprompts if the entered value is not in the valid range.

Example 1, Smart Card mode, with Echo on:

Online > A < Return >

First Officer:

Insert card and enter PIN: * * * * < Return >

Second Officer:

Insert card and enter PIN: * * * * * * < Return >

AUTHORIZED

Online - AUTH>

Example 2, Password mode, with Echo off:

Online > A < Return >

First Officer:

Password: * * * * * * * * * * * * * * < Return >

Second Officer:

Password: * * * * * * * * * * * * * * * * * * < Return > ← Password too long

NOT AUTHORIZED

Online >

3.2 Cancelling the Authorised State

Command	C (Can be used online and offline).
Function:	To cancel the Authorised state. The HSM responds NOT AUTHORIZED. (There is an equivalent command available to the Host). An HSM reset (performed by pressing the RESET button) also cancels the Authorised state.
Inputs:	None.
Outputs:	None.
Errors:	None.

Example:

Online - AUTH > C < Return >

NOT AUTHORIZED

Online >

4 VIEWING HSM STATUS INFORMATION

There are five 'Query' commands to display various settings in the HSM:

QA	:	Query Auxiliary
QC	:	Query Console
QH	:	Query Host
QS	:	Query Security (Detailed in Chapter 3)
VR	:	Version

4.1 Viewing HSM Auxiliary Port Configuration Information

Command	QA (Query Auxiliary).
Function:	To display details of the Auxiliary port configuration of the HSM.
Inputs:	None.
Outputs:	The Auxiliary port baud rate.
	The Auxiliary port word format.
	Flow control is fixed as XON/XOFF.
Errors:	None.

Example:

Online > QA < Return >

Baud: 9600
Word format: 7 bits, even parity, 1 stop
Flow control: XON/XOFF

4.2 Viewing HSM Console Port Configuration Information

Command:	QC (Query Console).
Function:	To display details of the Console port configuration of the HSM.
Inputs:	None.
Output:	The Console baud.
	The Console word format.
	Flow control is fixed as XON/XOFF.
Errors:	None.

Example:

Online > QC < Return >

Baud: 9600
Word format: 8 bits, no parity, 1 stop
Flow control: XON/XOFF

4.3 Viewing HSM Host Port Configuration Information

Command: QH (Query Host).

Function: To display details of the Host port configuration of the HSM.

Inputs: None.

Outputs: The message header length. This is the number of characters at the front of each command from the Host to the HSM (after the STX character). The HSM returns the message header in the response.

Whether the Host port is configured to be asynchronous, transparent asynchronous or bisynchronous.

In a bisynchronous system, the poll/select address. This is the address the HSM responds to when polled or selected.

In a bisynchronous IMS environment, the HSM searches for one or more strings in the message header to indicate that the data received is a valid transaction. The valid strings can be defined.

In a bisynchronous IMS system, the transaction test string offset. This is the number of characters into the message header from where the HSM starts to search for one of the valid transaction test strings.

In a bisynchronous system, whether the Host interface is configured to be DCE or DTE. The actual electrical connections must be configured as a DCE port.

In an asynchronous system, the response delay. This is the delay before the HSM responds to the Host. It allows use of half-duplex Host communications that require a defined delay between the transmission of a command and the response from the HSM.

In an SDLC or an SNA - SDLC synchronous system, whether the interface is DCE or DTE.

In an SDLC or an SNA - SDLC synchronous system, the IBM environment. This can be IMS or CICs. Message identifier and offset are shown.

In an SNA - SDLC synchronous system, the interface port type. This can be RS-232 or V.35.

In an SNA - SDLC synchronous system, the SDLC station address.

The Host baud.

The Host word format.

In Ethernet use, the IP address. This is the Internet Protocol address of the HSM in the system.

In Ethernet use, the Well-Known-Address. This is the publicised TCP Port address of the HSM.

Errors: None.

Example 1 (for transparent asynchronous communications):

Online > QH< Return >

Message header length: 04
Protocol: Transparent Asynchronous
Character format: ASCII
Terminating Sequence: 03 00
Interface: DCE
Response delay (ms): 00
Baud: 9600
Word format: 7 bits, no parity, 1 stop

Example 2 (for channel-attached communications):

Online > QH< Return >

Message header length: 04

Example 3 (for high speed SDLC communications):

Online > QH< Return >

Message header length: 08
Protocol: SDLC
Character format: ASCII
Station Address: 40
Interface: DCE
Baud: 224000
Word format: 8 bits, no parity

Example 4 (for SNA-SDLC communications):

Online > QH< Return >

Message header length: 08
Protocol: SNA/SDLC 3274
Mode: Normal
Character format: EBCDIC
Station Address: C1
Host environment: IMS
IMS message identifier: PIN,MAC
IMS identifier offset: 03
Interface: V.35, DCE
Baud: 64000
Word format: 8 bits, no parity

Example 5 (for Ethernet):

Online > QH< Return >

Message header length: 04
Protocol: Ethernet
Character format: ASCII
IP address: 128.100.3.1
Well-Known-Port address: 1500

4.4 Viewing the HSM Software Revision Number

Command: VR.

Function: To display details of the software release number, revision number and checksum.

Inputs: None.

Outputs: Software revision number and checksum.

Example:

Online > VR < Return >

Base release: 5.00
Revision: 9419 - E000
Checksum: FFE6

5 KEY MANAGEMENT FUNCTIONS

The HSM provides the following key management console commands:

- Generate a key component
- Generate a key component and write it to a smart card
- Encrypt a clear component
- Form a key from clear components
- Generate a key
- Import a key
- Export a key

The key type table shows the codes to use when selecting a key.

5.1 Key Type Table

LMK Pair / Variant	LMK Pair code	0	1	2	3	4	5	6	7	8	9
04-05	00	ZMK									
06-07	01	ZPK									
14-15	02	PVK TPK TMK				CSCK					
16-17	03	TAK									
18-19	04					CVK					
20-21	05	PVK (NOU)				CVK (NOU)					
22-23	06	WWK									
24-25	07	ZTK	KEK (CC)	CMK (CC)							
26-27	08	ZAK									
28-29	09	TDK BDK	MK-AC MK-SMI	MK-MAC MK-SMC	MK-ENC	KME MK-DFA MK-DAK	KMD MK-EE MK-DN	MK-DAC	MK-DN		
30-31	0A	ZEK ITK									
32-33	0B										
34-35	0C										
36-36	0D										
38-39	0E										

Notes:

NOU – Not on us
CC – Chip Card

Not all key type codes are available in all commands for security reasons.
The Key type code used within commands is formed by using the Variant code as the first character then the LMK pair code as the second character. For example the code for a ZPK is 001.

5.2 Key Scheme Table

Key Scheme Tag	Notes
Z	Single length DES key encrypted using ANSI X9.17 methods
U	Encryption of a double length key using variant method. Used for encryption of keys under LMK and can be used for import and export of keys.
T	Encryption of a triple length key using variant method. Used for encryption of keys under LMK and can be used for import and export of keys.
X	Encryption of a double length key using ANSI X9.17 methods only available for import and export of keys. This mode is enabled within configure security command
Y	Encryption of a triple length key using ANSI X9.17 methods only available for import and export of keys. This mode is enabled within configure security command

5.3 Generate Key Component

Command: GC (Can be used online and offline).

Function: To generate a key component and display it in plain and encrypted forms.

Inputs: Key length: (1 - Single length, 2 - Double Length, 3 -Triple Length).
Key Type: See key type table
Key Scheme: Key scheme for encrypting key under LMK see key scheme table
(Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Outputs: Clear text key component: 16 Hex or 32 or 48 hexadecimal characters.

key component encrypted under an appropriate variant of LMK:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.

Component check value; formed by encrypting 64 binary zeros with the component and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

Example:

Online > GC< Return >
Key length [1,2,3]: 1<Return>
Key Type: 001<Return>
Key Scheme: 0<Return>

Clear Component: XXXX XXXX XXXX XXXX
Encrypted Component: XXXX XXXX XXXX XXXX
Key check value: XXXX XX

5.4 Generate Key Components and write to Smart Card

Command: GS (Can be used online and offline).

Function: To generate a key in 2 to 9 component and write the components to smartcards.

The HSM must be in Authorised state

Inputs: Number of components, 1 numeric digit.
Key length: (1 - Single length, 2 - Double Length, 3 -Triple Length).
Key Type: See key type table
Key Scheme: Key scheme for encrypting key under LMK see key scheme table
(Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Outputs: Key encrypted under appropriate LMK:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex

Key Check value; formed by encrypting 64 binary zeros with the ZMK: 6 hexa decimal characters.

Errors: MASTER KEY PARITY ERROR. The contents of LMK storage have been erased. Do not continue. Inform the Security Department.

CARD NOT FORMATTED – the card does not have the appropriate file structure.

INVALID PIN; RE-ENTER – the entered PIN is not 4 – 8 digits.

PIN REJECTED BY CARD; RE-ENTER – self-explanatory.

WARNING – CARD CONTAINS A KEY COMPONENT; OVERWRITE? [Y/N]: - a key component already exists on the card.

DEVICE WRITE FAILED – the component could not be verified.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

NOT AUTHORISED - the HSM is not in Authorised state.

Example:

Online - AUTH > GS < Return >
Key length [1,2,3]: 1<Return>
Key Type: 001<Return>
Key Scheme: 0<Return>
Enter number of components [2-9]: 2<Return>
Insert card 1 and enter PIN: XXXX<Return>
Make additional copies? [Y/N]: N<Return>
Insert card 2 and enter PIN: XXXX<Return>
Make additional copies? [Y/N]<Return>

Encrypted key: XXXX XXXX XXXX XXXX
Key check value: XXXX XX
Online - AUTH>

5.5 Encrypt Clear Component

Command: EC(Can be used online and offline).

Function: To encrypt a clear text component and display the result at the Console.

The HSM must be in the Authorised state.

If the component does not have odd parity, odd parity will be forced before encryption

Inputs: Clear text key component: 16 or 32 or 48 hexadecimal characters.
Key Type: See key type table
Key Scheme: Key scheme for encrypting key under LMK see key scheme table
(Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Outputs: The key component encrypted under an appropriate variant of LMK:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.
Component check value; formed by encrypting 64 binary zeros with the component and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The input data does not contain 16 or 32 or 48 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

NOT AUTHORISED. The HSM is not in the Authorised state.

Example:

Online - AUTH > ?? < Return >
Key type: 001<Return>
Key Scheme: 0<Return>
Enter component: * * * * * * * * * * * * * * * * < Return >

Encrypted component: XXXX XXXX XXXX XXXX
Key check value: XXXX XX

5.6 Form Key from Components

Command: FK (Can be used online and offline).

Function: To build a key from components. If clear components used they will not be checked for parity, but odd parity will be forced on the final key before encryption under the LMK.

The HSM must be in the Authorised state.

Inputs: Key length: (1 - Single length, 2 - Double Length, 3 -Triple Length).

Key Type: See key type table

Key Scheme: Key scheme for encrypting key under LMK see key scheme table
(Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Component Type:
(X = Clear XOR, H = Clear Half or Third Key, E = Encrypted, S = Smart Card)

The number of key components to be entered: 1 to 9.

The key component.

For clear XOR components each key component must contain 16 or 32 or 48 hexadecimal characters.
For clear Half or Third Key components each key component must contain 8 or 16 hexadecimal characters.
For encrypted components each component must contain 16 Hex or 1 Alpha + 32 hex or 1 Alpha + 48 Hex.
For Smart Card components the components will be extracted from smart cards.

Outputs: The key formed by exclusive-ORing or concatenating the components, forcing odd parity and encrypting under the appropriate LMK pair.

The key check value, formed by encrypting a block of zeros with the key, and returning the first 24 bits: 6 hexadecimal characters.

Errors: NOT AUTHORISED. The HSM is not in the Authorised state.

DATA INVALID; PLEASE RE-ENTER - The amount of input data is incorrect. Re-enter the correct number of hexadecimal characters.

INVALID PIN; RE-ENTER – the entered PIN is not 4 – 8 digits.

PIN REJECTED BY CARD; RE-ENTER – self-explanatory.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example 1:

Online - AUTH > ?? < Return >
Key Length[1,2,3]: 2 <Return>
Key type: 002 <Return>
Key Scheme: U<Return>
Component type [X,H,E,S]: X <Return>
Enter number of components (2-9): 2 < Return >
Enter component 1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter component 2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZ

Example 2: Input from Smart Card

Online - AUTH > ?? < Return >
Key Length[1,2,3]: 2 <Return>
Key type: 002 <Return>
Key Scheme: U<Return>
Component type [X,H,E,S]: S <Return>
Enter number of components (2-9): 2 < Return >
Insert card 1 and enter PIN: XXXX < Return >
Insert card 2 and enter PIN: XXXX < Return >

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZ

Example 2: Form from encrypted components

Online - AUTH > ?? < Return >
Key Length[1,2,3]: 2 <Return>
Key type: 002 <Return>
Key Scheme: U<Return>
Component type [X,H,E,S]: E <Return>
Enter number of components (2-9): 2 < Return >
Enter component 1: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter component 2: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >

Encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZ

5.7 Generate Key

Command: KG (Can be used online and offline).

Function: To generate a random key and return it encrypted under the LMK and optionally under a ZMK (for transmission to another party).

Inputs: Key length: (1 - Single length, 2 - Double Length, 3 -Triple Length).

Key Type: See key type table

Key Scheme (LMK): Key scheme for encrypting key under LMK see key scheme table (Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Key Scheme (ZMK): Key scheme for encrypting key under ZMK see key scheme table (Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Optional ZMK encrypted under LMK pair 04-05 (as generated using the D or FK command): 16 Hex or 32 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex. (if <Return> at this prompt only key encrypted under LMK returned)

Optional ZMK key check value (as generated using the D or FK command or by extracting the first 6 digits generated using the CK command): 6 hexadecimal characters. (if <Return> at this prompt test not carried out)

Optional ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: The key encrypted under appropriate LMK pair:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.

Optionally the key encrypted under the ZMK:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex

The key check value, formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The encrypted ZMK does not contain the correct characters, or the key check value does not contain 6 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The ZMK does not have odd parity on each byte. Re-enter the encrypted ZMK and check for typographic errors.

KEY CHECK FAILED. The key check value for the ZMK does not match the key check value entered.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

MASTER KEY PARITY ERROR. The contents for LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > KG < Return >
Key Length[1,2,3]: 2 <Return>
Key type: 002 <Return>
Key Scheme(LMK): U<Return>
Key Scheme(ZMK): X<Return>
Enter encrypted ZMK: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter ZMK check value: XXXX XX< Return >
(Enter ZMK variant: X < Return >, if enabled by CS command)

Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key encrypted for transmission: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZ

Online > KG < Return >
Key Length[1,2,3]: 2 <Return>
Key type: 002 <Return>
Key Scheme(LMK): U<Return>
Key Scheme(ZMK):<Return>
Enter encrypted ZMK: < Return >

Key under LMK: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZ

5.8 Import Key

Command: IK(can be used online and offline).
The HSM must be in the Authorised state.

Function: To import a key from encryption under ZMK to encryption under LMK. If the key imported does not have odd parity a warning will be issued and odd parity will be forced on the key before encryption under the LMK.

Inputs: ZMK encrypted under LMK pair 04-05: 16 Hex or 32 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.

Key type: See key type table

Key Scheme: Key scheme for encrypting key under LMK see key scheme table
(Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Key encrypted under the ZMK: 16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex

ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: The key encrypted under appropriate LMK.
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.
If the key does not have odd parity the parity is corrected and warning issued.

The key check value, formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: NOT AUTHORIZED.

INVALID - Incorrect input data length.

ZMK PARITY ERROR.

KEY PARITY WARNING.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

MASTER KEY PARITY ERROR.

Example:

Online - AUTH > KI < Return >
Key type: 002 < Return >
Key Scheme: U<Return>
Enter ZMK: aaaa aaaa aaaa aaaa bbbb bbbb bbbb bbbb < Return >
(Enter ZMK variant: X < Return >, if enabled by CS command)
Enter key : X XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >

Key under LMK: U MMMM MMMM MMMM MMMM MMMM MMMM MMMM MMMM
Key Check Value: NNNN NN

5.9 Export Key

Command: KE (Can be used online and offline).

Function: To translate a key from encryption under the LMK to encryption under a ZMK.

The HSM must be in the Authorised state.

Inputs: ZMK encrypted under LMK pair 04-05: 16 Hex or 32 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex.

Key type: See key type table

Key Scheme (ZMK): Key scheme for encrypting key under ZMK see key scheme table (Defaults: Key length 1, Key Scheme 0,
Key Length 2, Key Scheme U,
Key Length 3, Key Scheme T)

Key encrypted under the appropriate LMK:
16 Hex or 1 Alpha + 32 Hex or 1 Alpha + 48 Hex

The ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: The key encrypted under the ZMK: 16 hex, 1 alpha + 32 hex or 1 alpha + 48 hex.

The key check value: formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The encrypted ZMK does not contain 16 or 32 hex or 1 alpha + 32 hex or 1 alpha + 48 hex. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The ZMK or ZPK does not have odd parity on each byte. Re-enter the key and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the security department.

INVALID KEY SCHEME FOR KEY LENGTH. The Key scheme is inappropriate for Key length.

NOT AUTHORIZED. The HSM is not in the Authorised state.

Example:

Online -AUTH > KE < Return >
Key type: 002 < Return >
Key Scheme (ZMK): X<Return>
Enter encrypted ZMK: T XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
(Enter ZMK variant: X < Return >, if enabled by CS command)
Enter encrypted key: U YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY < Return >

Key encrypted under ZMK: X YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: XXXX XX

6 ZONE MASTER KEY FUNCTIONS

The HSM provides Console commands to generate and form Zone Master Keys (ZMKs) by components.

To form a ZMK requires at lease two components. For security reasons, the components must be encrypted under one of the LMK pairs before the HSM accepts them and forms the ZMK. Therefore the HSM provides facilities to:

Generate a clear text component and its encrypted form.
Encrypt a clear text component (for components received from another institution).
Combine a number of encrypted components.

6.1 Generating a Zone Master Key Component

Command:	F (Can be used online and offline).
Function:	To generate a ZMK component and display it in plain and encrypted forms.
Inputs:	None.
Outputs:	Clear text ZMK component: 16 or 32 hexadecimal characters. ZMK component encrypted under a variant of LMK pair 04-05: 16 or 32 hexadecimal characters. Component check value; formed by encrypting 64 binary zeros with the component and returning the left-most 24 bits: 6 hexadecimal characters.
Errors:	MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > F < Return >

Clear ZMK Component: XXXX XXXX XXXX XXXX
Encrypted ZMK Component: XXXX XXXX XXXX XXXX
Key check value: XXXX XXXX XXXX XXXX

6.2 Generate a Zone Master key, Write Components to Smartcards

Command: GZ (Can be used online and offline).

Function: To generate a ZMK in 2 to 9 component and write the components to smartcards.

The HSM must be in Authorised state

Inputs: Number of components, 1 numeric digit.

Outputs: ZMK encrypted under LMK pair 04-05 : 16 or 32 hexadecimal characters.

ZMK Check value; formed by encrypting 64 binary zeros with the ZMK; 16 hexadecimal characters.

Errors: MASTER KEY PARITY ERROR. The contents of LMK storage have been erased. Do not continue. Inform the Security Department.

CARD NOT FORMATTED – the card does not have the appropriate file structure.

INVALID PIN; RE-ENTER – the entered PIN is not 4 – 8 digits.

PIN REJECTED BY CARD; RE-ENTER – self-explanatory.

WARNING – CARD CONTAINS ZMK COMPONENT; OVERWRITE? [Y/N]: - a ZMK component already exists on the card.

DEVICE WRITE FAILED – the component could not be verified.

NOT AUTHORISED - the HSM is not in Authorised state.

Example:

Online - AUTH > GZ < Return >

Enter number of components [2-9]: <Return>

Insert card 1 and enter PIN: XXXX<Return>

Make additional copies? [Y/N]: N<Return>

Insert card 2 and enter PIN: XXXX<Return>

Make additional copies? [Y/N]<Return>

Encrypted ZMK: XXXX XXXX XXXX XXXX

Key check value: XXXX XXXX XXXX XXXX

Online - AUTH>

6.3 Encrypting a Clear Zone Master Key Component

Command: Z (Can be used online and offline).

Function: To encrypt a clear text component and display the result at the Console.

The HSM must be in the Authorised state.

Inputs: Clear text ZMK component: 16 or 32 hexadecimal characters.

Outputs: The ZMK component encrypted under a variant of LMK pair 04-05: 16 or 32 hexadecimal characters.

Component check value; formed by encrypting 64 binary zeros with the component and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The input data does not contain 16 or 32 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The entered component does not have odd parity on each byte. Ensure the component has odd parity and re-enter.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

NOT AUTHORIZED. The HSM is not in the Authorised state.

Example:

Online - AUTH > Z < Return >

Enter ZMK Component: * * * * * * * * * * * * * * * * < Return >

Encrypted ZMK Component: XXXX XXXX XXXX XXXX

Key check value: XXXX XXXX XXXX XXXX

6.4 Forming a Zone Master Key From Encrypted Components

Command: D (Can be used online and offline).

Function: To form a ZMK from encrypted components. The components may either be entered from the console or read from smartcards.

The manually entered components must have been encrypted using the Z command, or generated using the F command.

The HSM must be in the Authorised state.

Inputs: Type of input, Smartcard or keyboard

The number of key components to be entered: 2 to 9.

The ZMK components, each encrypted under a variant of LMK pair 04-05: 16 hexadecimal characters.

Outputs: The ZMK encrypted under LMK 04-05: 16 or 32 hexadecimal characters.

The key check value, formed by encrypting 64 binary zeros with the ZMK, and returning all 64 bits: 16 hexadecimal characters.

Errors: NOT AUTHORISED. The HSM is not in the Authorised state.

INVALID. The input data does not contain 16 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The entered component does not have odd parity on each byte. Re-enter the encrypted component and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example 1: Input from console

Online - AUTH > D < Return >

Input components from smartcards? [Y/N]: N<Return>

Enter number of components (2-9): 2 < Return >

Enter encrypted component 1: XXXXXXXXXXXXXXXX < Return >

Enter encrypted component 2: XXXXXXXXXXXXXXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY

Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

Example 2: Input from Smart Card

Online - AUTH > D < Return >

Input components from smartcards? [Y/N]: N<Return>

Enter number of components (2-9): 2 < Return >

Insert card 1 and enter PIN: XXXX < Return >

Insert card 2 and enter PIN: XXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY

Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

6.5 Importing a CVK or PVK from ZMK to LMK

Command: IV (can be used online and offline).
The HSM must be in the Authorised state.

Function: To import VISA PVK or CVK from encryption under ZMK to encryption under LMK.

Inputs: ZMK encrypted under LMK pair 04-05: 16 or 32 hexadecimal characters.
Key type: C or P (for CVK or PVK respectively).

Key A and B encrypted under the ZMK: 16 hexadecimal characters.

ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: Key A and B encrypted under LMK 14-15 or variant: 16 hexadecimal characters.
Key check value: 6 hexadecimal characters.

Errors: NOT AUTHORIZED.
INVALID - Incorrect input data length.
ZMK PARITY ERROR.
VISA KEY PARITY ERROR.
MASTER KEY PARITY ERROR.

Example:

Online - AUTH > IV < Return >

Key type [Pvk/Cvk]: C < Return >

Enter ZMK: aaaa aaaa aaaa aaaa bbbb bbbb bbbb bbbb < Return >

(Enter ZMK variant: X < Return >, if enabled by CS command)

Enter key A: XXXXXXXXXXXXXXXX < Return >

Enter key B: YYYYYYYYYYYYYYYY < Return >

Key A under LMK: MMMM MMMM MMMM MMMM

Key Check Value: NNNN NNNN NNNN NNNN

Key B under LMK: MMMM MMMM MMMM MMMM

Key check value: NNNN NNNN NNNN NNNN

7 ZONE PIN KEY FUNCTIONS

The HSM provides Console commands to generate and translate Zone PIN keys (ZPKs).

7.1 Generating a Zone PIN Key (VISA Acquirer or Issuer Working Key)

Command: B (Can be used online and offline).

Function: To generate a random ZPK and return it encrypted under the LMK and under a ZMK (for transmission to another party).

Inputs: The ZMK (VISA Zone Control Master Key, ZCMK) encrypted under LMK pair 04-05 (as generated using the D command): 16 or 32 hexadecimal characters.

The ZMK key check value (as generated using the D command or by extracting the first 6 digits generated using the CK command): 6 hexadecimal characters.

The ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: The ZPK encrypted under the ZMK: 16 hexadecimal characters.

The ZPK encrypted under LMK pair 06-07: 16 hexadecimal characters.

The ZPK check value, formed by encrypting 64 binary zeros with the ZPK and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The encrypted ZMK does not contain 16 or 32 hexadecimal characters, or the key check value does not contain 6 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The ZMK does not have odd parity on each byte. Re-enter the encrypted ZMK and check for typographic errors.

MASTER KEY PARITY ERROR. The contents for LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > B < Return >

Enter encrypted ZMK: XX XX XX XX XX XX XX XX < Return >

Enter ZMK check value: XX XX XX< Return >

(Enter ZMK variant: X < Return >, if enabled by CS command)

ZPK encrypted for transmission: XXXX XXXX XXXX XXXX

ZPK encrypted for bank: XXXX XXXX XXXX XXXX

Key check value: XX XX XX

7.2 Translating a Zone PIN Key

Command: WK (Can be used online and offline).

Function: To translate a ZPK from encryption under the LMK to encryption under a ZMK.

The HSM must be in the Authorised state.

Inputs: ZMK encrypted under LMK pair 04-05: 16 or 32 hexadecimal characters.

The ZPK encrypted under LMK pair 06-07: 16 hexadecimal characters.

The ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: The ZPK encrypted under the ZMK: 16 hexadecimal characters.

The key check value for the ZPK; generated by encrypting 64 binary zeros with the key: 16 hexadecimal characters.

Errors: INVALID. The encrypted ZMK does not contain 16 or 32 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

PARITY ERROR. The ZMK or ZPK does not have odd parity on each byte. Re-enter the key and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the security department.

NOT AUTHORIZED. The HSM is not in the Authorised state.

Example:

Online -AUTH > WK < Return >

Enter encrypted ZMK: XX XX XX XX XX XX XX XX < Return >

(Enter ZMK variant: X < Return >, if enabled by CS command)

Enter encrypted WK: XX XX XX XX XX XX XX XX < Return >

ZPK encrypted under ZMK: XXXX XXXX XXXX XXXX

Key check value: XXXX XXXX XXXX XXXX

8 TERMINAL KEY FUNCTIONS

The HSM provides Console commands to encrypt existing clear text keys for use in local (terminal) networks.

8.1 Encrypting a Key Under LMK Pair 14-15

Command: K (Can be used online and offline).

Function: To form and encrypt a TMK, TPK or PVK under LMK 14-15. The TMK, TPK or PVK can be entered as a number of components in the range 1 to 9 inclusive.

The HSM must be in the Authorised state.

To ensure that the clear key is not displayed on the screen, enter the ^ character before entering the key component.

The entered components need not have odd parity, although the final TMK, TPK or PVK has odd parity.

Inputs: The number of key components to be entered: 1 to 9.

The clear key component. Each key component must contain 16 hexadecimal characters.

Outputs: The TMK, TPK or PVK encrypted under LMK 14-15: 16 hexadecimal characters.

The key check value, formed by encrypting a block of zeros with the TMK, TPK or PVK, and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: NOT AUTHORIZED. The HSM is not in the Authorised state.

INVALID NUMBER OF COMPONENTS. The number of components is not in the range 1 to 9. Re-enter the number of components.

INVALID KEY COMPONENT. The enter key component does not contain 16 hexadecimal characters. Re-enter the key component.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online - AUTH > K < Return >

Enter number of components (1-9): 2 < Return >

Enter component 1: XXXXXXXXXXXXXXXX < Return >

Enter component 2: XXXXXXXXXXXXXXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY

Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

9 KEY COMPONENT FUNCTIONS

The HSM provides console commands to build a key from clear components. The components will not be checked for parity, but odd parity will be forced on the final key before encrypting under the LMK. The length of the key is a function of type:

Type "0" (Base Derivation key):	32 Hexadecimal Characters
Type "1" (Card Verification Key):	16 Hexadecimal Characters
Type "2" (Zone PIN Key):	16 Hexadecimal Characters

9.1 Form a Key from Components

Command: BK (Can be used online and offline).

Function: To build a key from clear components. The components will not be checked for parity, but odd parity will be forced on the final key before encryption under the LMK.

The HSM must be in the Authorised state.

Inputs: Key Type; 1 numeric digit:
"0" - Base Derivation Key (BDK)
"1" - Card Verification Key (CVK)
"2" - Zone PIN Key (ZPK)

The number of key components to be entered: 2 to 9.

The clear key component. Each key component must contain 16 or 32 hexadecimal characters.

Outputs: The key formed by exclusive-ORing the entered components, forcing odd parity and encrypting under the appropriate LMK pair:
Key type "0" - LMK pair 28 - 29, 32 hexadecimal digits.
Key type "1" - LMK pair 14 - 15 variant 4, 16 hexadecimal digits.
Key type "2" - LMK pair 06 - 07, 16 hexadecimal digits.

The key check value, formed by encrypting a block of zeros with the key, and returning all 64 bits: 16 hexadecimal characters.

Errors: NOT AUTHORIZED. The HSM is not in the Authorised state.

DATA INVALID; PLEASE RE-ENTER - The amount of input data is incorrect. Re-enter the correct number of hexadecimal characters.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example 1: Form a *BDK from components

Online - AUTH > BK < Return >

Enter key type [0=BDK, 1=CVK, 2=ZPK]: 0 <Return>
Enter number of components (2-9): 2 < Return >
Enter component 1: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter component 2: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

Example 2: Form a CVK from components

Online - AUTH > BK < Return >

Enter key type [0=BDK, 1=CVK, 2=ZPK]: 1 <Return>
Enter number of components (2-9): 3 < Return >
Enter component 1: XXXX XXXX XXXX XXXX < Return >
Enter component 2: XXXX XXXX XXXX XXXX < Return >
Enter component 3: XXXX XXXX XXXX XXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

Example 3: Form a ZPK from components

Online - AUTH > BK < Return >

Enter key type [0=BDK, 1=CVK, 2=ZPK]: 2 <Return>
Enter number of components (2-9): 2 < Return >
Enter component 1: XXXX XXXX XXXX XXXX < Return >
Enter component 2: XXXX XXXX XXXX XXXX < Return >

Encrypted key: YYYY YYYY YYYY YYYY
Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

10 GENERATING A CHECK VALUE

Command: CK (Can be used online and offline).

Function: To generate a key check value (KCV) for a key encrypted under a specified LMK pair.

Inputs: Encrypted key (under the relevant LMK pair):

Single-length key: 16 hexadecimal characters.
Double-length key: 32 hex characters or 1 alpha + 32 hex characters.
Triple-length key 1 alpha + 48 hex

Key-Type: a code indicating the type of key that is to be input: 2 decimal digits:

Code	Key-Type
000	LMK pair 04-05
001	LMK pair 06-07
002	LMK pair 14-15
003	LMK pair 16-17
004	LMK pair 18-19
005	LMK pair 20-21
006	LMK pair 22-23
007	LMK pair 24-25
008	LMK pair 26-27
009	LMK pair 28-29
00A	LMK pair 30-31
00B	LMK pair 32-33
100	Variant 1 of LMK pair 04-05
402	Variant 4 of LMK pair 14-15
405	Variant 4 of LMK pair 20-21

Outputs: The check value: 16 hexadecimal characters.

Errors: INVALID KEY TYPE: Re-enter the correct value.

INVALID DATA INPUT: Re-enter the correct number of characters.

KEY PARITY ERROR. The entered key does not have odd parity on each byte. Re-enter the complete line (key and Key-Type code) and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > CK < Return >

Enter key type code: NNN < Return >
Enter key length flag [S/D/T]: S < Return >
or
D < Return >
or
T < Return >

Enter encrypted key: XXXX XXXX XXXX XXXX < Return >

or
YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY < Return >

or
T YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY
(as applicable)

Key check value: ZZZZ ZZZZ ZZZZ ZZZZ

11 CARD VERIFICATION KEY MANAGEMENT

The HSM provides Console commands to support the management of CVK pairs:

- Generate a CVK pair.
- Translate a CVK pair from encryption under a variant of an LMK to encryption under a ZMK.
- Translate a CVK pair from encryption under a ZMK to encryption under a variant of an LMK.

11.1 Generating a CVK Pair

Command: KA (can be used online and offline).

Function: To generate a CVK pair and output the key encrypted under a variant of LMK pair 14-15.

Inputs: None.

Outputs: CVK A encrypted under a variant of LMK pair 14-15: 16 hexadecimal characters.

The key check value for CVK A; formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

CVK B encrypted under a variant of LMK pair 14-15: 16 hexadecimal characters.

The key check value for CVK B; formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

Error: MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > KA < Return >

Encrypted CVK A: XXXX XXXX XXXX XXXX
Key check value: YYYYYY
Encrypted CVK B: XXXX XXXX XXXX XXXX
Key check value: YYYYYY

11.2 Translating a CVK Pair from Encryption Under the LMK to Encryption Under a ZMK

Command: KB (can be used online and offline).

Function: To translate a CVK pair from encryption under a variant of LMK pair 14-15 to encryption under a ZMK.

Inputs: CVK A encrypted under a variant of LMK pair 14-15: 16 hexadecimal characters.

CVK B encrypted under a variant of LMK pair 14-15: 16 hexadecimal characters.

ZMK encrypted under LMK pair 04-05: 16 or 32 hexadecimal characters.

The ZMK variant: 1 or 2 digit, value 0-99 (or <Enter> to ignore). Used only when interworking with Atalla systems. Refer to the CS command. Note that this input is not requested when the ZMK variant support is set to off.

Outputs: CVK A encrypted under the ZMK.

The key check value for CVK A, formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

CVK B encryption under the ZMK.

The key check value for CVK B, formed by encrypting 64 binary zeros with the key and returning the left-most 24 bits: 6 hexadecimal characters.

Errors: INVALID. The encrypted key does not contain the correct number of hexadecimal characters. Re-enter the key.

PARITY ERROR. The key does not have odd parity on each byte. Re-enter the key and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > KB < Return >

Enter encrypted CVK A: XXXX XXXX XXXX XXXX< Return >

Enter encrypted CVK B: XXXX XXXX XXXX XXXX< Return >

Enter encrypted ZMK: XXXX XXXX XXXX XXXX< Return >

(Enter ZMK variant: X < Return >, if enabled by CS command)

Encrypted CVK A: XXXX XXXX XXXX XXXX
Key check value: YYYYYY

Encrypted CVK B: XXXX XXXX XXXX XXXX
Key check value: YYYYYY

12 VISA VERIFICATION FUNCTIONS

The HSM provides console commands to generate VISA card and PIN verification values.

12.1 Generating a VISA Card Verification Value

Command: CV (Can be used online and offline).
The HSM must be in the Authorised state.

Function: To generate a VISA card verification value (CVV).

Inputs: Encrypted CVK A under a variant of LMK pair 14-15: 16 hexadecimal characters.

Encrypted CVK B under a variant of LMK pair 14-15: 16 hexadecimal characters.

The CVK can be presented as a double length key using the new scheme.

Primary account number (PAN) for the card: up to 19 decimal digits.

Card Expiry date: 4 decimal digits.

Service code: 3 decimal digits.

Outputs: Card Verification Value: 3 decimal digits.

Errors: NOT AUTHORIZED.

INVALID - Incorrect input data length.

PARITY ERROR.

MASTER KEY PARITY ERROR.

Example:

Online - AUTH > CV < Return >

Enter key A: XXXXXXXXXXXXXXXX < Return >
Enter key B: YYYYYYYYYYYYYYYY < Return >
Enter PAN: 1234567812345678 < Return >
Enter expiry date: 0694 < Return >
Enter service code: 123 < Return >
CVV: 123

Example:

Online - AUTH > CV < Return >

Enter key A: U XXXX XXXX XXXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter PAN: 1234567812345678 < Return >
Enter expiry date: 0694 < Return >
Enter service code: 123 < Return >
CVV: 123

12.2 Generating a VISA Pin Verification Value

Command: PV (Can be used online and offline).

Function: To generate a VISA PIN Verification Value (PVV).

The HSM must be in the Authorised state.

Inputs: Encrypted PVK A under LMK pair 14-15: 16 hexadecimal characters.

Encrypted PVK B under LMK pair 14-15: 16 hexadecimal characters.

The CVK can be presented as a double length key using the new scheme.

The PVV data block comprising:

The 11 right-most digits of the account number (excluding check digital): 11 decimal digits.

The PIN verification key indicator (PVKI): 1 decimal digit.

The 4 left-most digits of the clear PIN: 4 decimal digits.

Outputs: The PIN Verification Value (PVV): 4 decimal digits.

Errors: NOT AUTHORIZED. The HSM is not in the Authorised state.

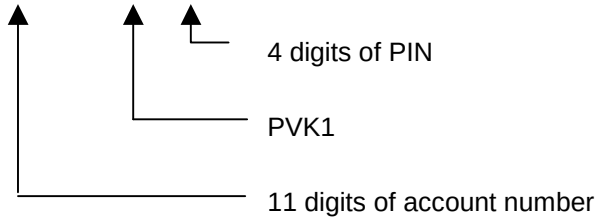
INVALID. The PVK A, PVK B or the PVV data block field is not 16 characters long. Re-enter the correct number of characters.

PARITY ERROR. PVK A or PVK B does not have odd parity on each byte. Re-enter the encrypted PVK A or PVK B and check for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online - AUTH > PV <Return>
Enter key A: XXXX XXXX XXXX XXXX <Return>
Enter key B: XXXX XXXX XXXX XXXX <Return>
Enter PVV data block: XXXXXXXXXXX N NNNN <Return>
PVV: NNNN



Online - AUTH > PV <Return>
Enter key A: U XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX <Return>
Enter PVV data block: XXXXXXXXXXX N NNNN <Return>
PVV: NNNN

13 LOADING THE DIEBOLD TABLE

Command: R (Online only).

Function: To load the Diebold table into user storage in the HSM.

The HSM must be in the Authorised state.

Inputs: Location in user storage at which to store the Diebold table. This value must be between 0 and 5E0 (hexadecimal). Ensure that the location of the table does not conflict with any other previously-defined storage area: 3 hexadecimal characters.

Diebold Table: 512 hexadecimal characters (entered as 32 sets of 16 characters).

Outputs: The 512-character encrypted table: 16 lines of 32 hexadecimal characters each.

Errors: INVALID INDEX. The specified location in user storage is out of range. Enter a valid value.

INVALID. The entered index is not 3 hexadecimal characters long, or a table entry is not 16 hexadecimal characters long. Re-enter the correct number of hexadecimal characters.

INVALID TABLE. Some of the data entered is not a valid entry for a Diebold table. Check the table and re-enter the data, checking for typographic errors.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

NOT AUTHORIZED. The HSM is not in the Authorised state.

Example:

Online - AUTH > R < Return >

Enter index (000 - 5FF): XXX < Return >
Now enter table, 16 hex digits/line

Line 01: XXXX XXXX XXXX XXXX < Return >
XXXX XXXX XXXX XXXX OK? [Y/N] Y < Return > (Y must be upper case)

Line 02:
etc.

Line 32: XXXX XXXX XXXX XXXX < Return >
XXXX XXXX XXXX XXXX OK? [Y/N] Y< Return > (Y must be upper case)

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

etc.

XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

(16 lines of encrypted table are displayed).

14 DUKPT CONSOLE COMMANDS

The Derived Unique Key Per Transaction system accesses the following commands via the terminal attached to the HSM:
Generate a double-length *ZMK component.
Form a *ZMK from clear components.
Import a Base Derivation Key.
Generate a Base Derivation Key.

14.1 Generate a Double-Length *ZMK Component

Command: DD.

Function: To generate a double-length random *ZMK component and display the value at the Console screen. The command ignores the S/D (single/double length) parameter set by the CS (Configure Security) command.

Inputs: None.

Outputs: The clear *ZMK component.

Errors: MASTER KEY PARITY ERROR. The LMK storage has been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > DD <Return>

Clear *ZMK component: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

14.2 Form a *ZMK from Clear Components

Command DE.

Function: To enter a *ZMK as either two single-length components (halves) or as two to nine double-length components.

Notes: The DE command differs from the D command as follows:

- It uses clear components (not encrypted components).
- It forms the *ZMK from two 16-character halves, or from two to nine 32-character components.

When H/F is set to H, two 16-character halves are used: the user is prompted to enter 16 left characters, then 16 right characters. (The unit concatenates the left and right halves).

When H/F is set to F, two to nine 32-character components are used: the user is prompted to enter the first component, then the second component, then the third, etc., according to the number of components to be entered. (The unit exclusive-OR combines the 32-character components).

The parity of the components is not checked, but the resulting *ZMK has odd parity forced before encryption.

The HSM must be in the Authorised state.

If the Echo parameter entered in the CS (Configure Security) command has been set to N (on), the clear components are echoed onto the screen as they are entered. If this is not required, either:

- Use the CS command to set the Echo parameter to F (off);
  or
- Enter ∧ (i.e. press the Shift and 6 keys) before entering each component.

Inputs: A half-length or full-length flag.
The number of components
The clear components: each 16 or 32 hexadecimal characters.

Outputs: The *ZMK encrypted under LMK pair 04-05.
The key check value (KCV) for the *ZMK.

Errors: INVALID. The input data does not contain 16 or 32 hexadecimal characters. Re-enter the correct number of hexadecimal characters.
MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.
NOT AUTHORISED. The HSM is not in the Authorised state.

Example, using two single-length components (halves):

Online - AUTH > DE <Return>
Half or full-length components? (H/F): H <Return>
Enter left component: xxxx xxxx xxxx xxxx <Return>
Enter right component: xxxx xxxx xxxx xxxx <Return>
Encrypted ZMK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Key check value: xxxx xxxx

Example, using two to nine double-length components:

Online - AUTH > DE <Return>

Half or full-length components? (H/F): F <Return>
Enter number of clear components: 3 <Return>
Enter first component: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx <Return>
Enter second component: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx <Return>
Enter third component: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx <Return>
Encrypted ZMK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Key check value: xxxx xxxx

14.3 Import a Base Derivation Key (*BDK)

Command: DF

Function: To import a BDK encrypted under a *ZMK and translate it to encryption under LMK pair 28-29.

Notes: A KCV for the *BDK is also computed and displayed.
The command also prompts for a variant. If the exporter applied a variant to the *ZMK, enter the variant number.

Inputs: *ZMK encrypted under LMK pair 04-05: 32 hexadecimal characters.
*ZMK variant (or <Return> to ignore). (The command ignores the setting of the Atalla ZMK variant support parameter entered in the CS (Configure Security) command).
*BDK encrypted under the ZMK: 32 hexadecimal characters.

Outputs: *BDK encrypted under LMK pair 28-29.
*BDK, KCV.

Errors: KEY PARITY ERROR. The entered key does not have odd parity. Re-enter the key and check for typographic errors.
MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > DF <Return>

Enter *ZMK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Enter *ZMK variant: x
Enter *BDK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Encrypted *BDK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Key check value: xxxx xxxx

14.4 Generate a Base Derivation Key (*BDK)

Command: DG (equivalent to Host BI command).

Function: To generate a random *BDK, displaying it encrypted under the LMK pair and under a *ZMK, and a *BDK check value.

Notes: The command also prompts for a variant. If the recipient requires a variant to the *ZMK, enter the appropriate variant number.

Inputs: *ZMK encrypted under LMK pair 04-05 (generated by the DE command): 32 hexadecimal characters.
*ZMK variant (or <Return> to ignore). (The command ignores the setting of the Atalla ZMK variant support parameter entered in the CS (Configure Security) command).
*ZMK key check value (generated by the DE command) or the value generated by the Console CK command or Host BU command.

Outputs: *BDK encrypted under the *ZMK: 32 hexadecimal characters.
*BDK encrypted under LMK pair 28-29: 32 hexadecimal characters.
*BDK check value.

Errors: INVALID. The encrypted *ZMK does not contain 32 hexadecimal characters or the key check value does not contain 8 hexadecimal characters. Re-enter the correct number of hexadecimal characters.
PARITY ERROR. The entered *ZMK does not have odd parity on each byte. Re-enter the encrypted *ZMK and check for typographic errors.
CHECK KEY FAILURE. THE *ZMK check key value is not correct. Re-enter the correct check value.
MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > DG <Return>

Enter encrypted *ZMK: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx <Return>
Enter *ZMK variant, 1 numeric digit or <Return>: x <Return>
Enter *ZMK check value: xxxx xxxx <Return>
*BDK encrypted for transmission : xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
*BDK encrypted under LMK 28-29: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
Key check value: xxxx xxxx

15 DIAGNOSTIC TEST

Command: DT (Offline only).

Function: To perform diagnostic tests.

The DT command tests the following parts of the HSM:

Working memory areas (RAM).

Program code (firmware in PROM).

The DES cryptographic processor.

Smart Card reader operation.

DSP cryptographic processor and its boot PROM firmware.

Battery voltage level.

Inputs: None.

Outputs: PASS or FAIL messages.

Example:

Online > DT < Return >

Memory test ... OK
Firmware test ... OK
DES test ... OK
Check smart card eject ...
DSP test ... OK
Battery ... OK
DIAGNOSTICS COMPLETE

16 DES CALCULATOR

The HSM provides two commands to encrypt and decrypt data with a known key. This provides the facilities of a simple DES calculator.

- To encrypt and decrypt with a single-length key.
- To encrypt and decrypt with double-length key.

16.1 Single-Length Key Calculator

Command: N [16-character key] [16-character data block].

(Can be used online and offline).

Function: To encrypt and decrypt the given data block with the given single-length key.

Inputs: Key (no parity required): 16 hexadecimal characters.

Data block: 16 hexadecimal character.

Outputs: The data encrypted with the key.

The data decrypted with the key.

Errors: INVALID. The entered data does not comprise 32 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

Example:

Online > N < Return >

Enter key: XXXXXXXXXXXXXXXX < Return >
Enter data: XXXXXXXXXXXXXXXX < Return >
Encrypted: XXXX XXXX XXXX XXXX
Decrypted: XXXX XXXX XXXX XXXX

16.2 Double-Length Key Calculator

Command: $ [32-character key] [16-character data block].
(Can be used online and offline).

Function: To encrypt and decrypt the given data block with the given double-length key.

Inputs: The double-length key (odd parity is required): 32 hexadecimal characters.
Data block: 16 hexadecimal characters.

Outputs: The data encrypted with the key.

The data decrypted with the key.

Errors: INVALID. The entered data does not comprise 48 hexadecimal characters. Re-enter the correct number of hexadecimal characters.

KEY PARITY ERROR. The entered key does not have correct parity. Check the parity and re-enter the command.

Example:

Offline > $ < Return >

Enter key: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX < Return >
Enter data: XXXXXXXXXXXXXXXX < Return >
Encrypted: XXXX XXXX XXXX XXXX Decrypted: XXXX XXXX XXXX XXXX

17 SMART CARDS

The HSM provides Console commands to support the use of Smart Cards:

- Format a Smart Card.
- Create an Authorizing Officer Smart Card.
- Verify the contents of a Smart Card.
- Change a Smart Card PIN.
- Import a CVK or PVK from ZMK to LMK.
- Read Smart Card Details (unidentifiable card).
- Copy a PROM to a Smart Card.

If a Smart Card function returns an error message code in the form:
XX XX

note the value displayed and contact the local HSM service provider.

NOTE: DO NOT REPEATEDLY ENTER INVALID PINS. A CARD "LOCKS" AFTER SEVEN INVALID PINS HAVE BEEN ENTERED, AND IT CAN BE "UNLOCKED" ONLY BY REFORMATTING, WHICH DELETES THE ENTIRE CONTENTS OF THE CARD.

17.1 Formatting a Smart Card

Command: FC (can be used online and offline).

Function: To format a Smart Card for use by the HSM.

A standard format is used for local storage and basic RSA functions.

Inputs: Smart Card PIN: 4 to 8 alphanumeric characters.
Date: 6 numeric character format DDMMYY.
Time: 6 numeric characters; format hhmmss.
Issuer ID: maximum 35 alphanumeric characters.
User ID: maximum 35 alphanumeric characters.

Outputs: Text messages:
Insert Card and press ENTER when ready.
Enter new PIN for Smart Card.
Re-enter new PIN.
Enter format code.
Enter date.
Enter time.
Enter Issuer ID.
Enter User ID.
FORMAT CODE NOT AVAILABLE.
WARNING CARD ALREADY FORMATTED, CONTINUE? [Y/N]. FORMAT COMPLETE.

Example:

Online > FC < Return >

Insert Smart Card and press ENTER: < Return >
WARNING CARD ALREADY FORMATTED, CONTINUE? [Y/N]: Y< Return
Erasing card
Formatting card . . .
Enter new PIN for Smart Card: * * * * * * * < Return >
Re-enter new PIN: * * * * * * * < Return >
Enter time [hhmmss]: 153540< Return >
Enter date [DDMMYY]: 261093< Return >
Enter User ID: Joe Small< Return >
Enter Issuer ID: Big Bank plc< Return >
FORMAT COMPLETE
Online>

17.2 Creating an Authorising Officer Smart Card

Command: CO (offline only).

Function: To copy the Password for an Authorising Officer to another Smart Card so that it can be used to set the HSM into the Authorised state.

Inputs: Smart Card PIN: 4 to 8 alphanumeric characters.

Outputs: Text messages:
Insert Card for Component Set 1 or 2 and enter the PIN.
Insert Card for Authorising Officer and enter the PIN.
PIN REJECTED BY CARD.
NOT AN LMK CARD OR CARD NOT FORMATTED.
CARD BLANK.
CARD NOT BLANK.
COPY COMPLETE.
COPY FAILED.
CARD DATA INVALID.

Example:

Online > CO < Return >

Insert Card for Component Set 1 or 2 and enter the PIN: * * * * * < Return >
Insert Card for Authorising Officer and enter the PIN: * * * * * < Return >

CARD NOT BLANK.
COPY FAILED.

17.3 Verifying the Contents of a Smart Card

Command: VC (can be used online and offline).

Function: To verify the contents of the Smart Cards held by a Component Holder. The HSM reads the LMK Component Set from the Smart Card, computes the check value, compares this with the check value stored on the card and displays the result.

Inputs: Smart Card PIN: 4 to 8 alphanumeric characters.

Outputs: Component Set check value: 16 hexadecimal characters.
Comparison: Pass or Fail.
Text messages:
NOT AN LMK CARD OR CARD NOT FORMATTED.
Master key check = .
Compare with card.

Example:

Online > VC < Return >

Insert Card and enter the PIN: * * * * * < Return >
Master key check = 0123 4567 89AB CDEF.
Compare with card: Pass.

If a Smart Card (or PROM) is defective or cannot be successfully verified, replace it. Copy a verified Smart Card (from the same set of components) onto a replacement, as described in Chapter 4. (In the case of a PROM, copy it in the equipment that originally produced the PROM).
NOTE: DISPOSE OF THE FAULTY SMART CARD (OR PROM) IN A SECURE MANNER.

17.4 Changing a Smart Card PIN

Command: NP (can be used online and offline).

Function: To select a new PIN for a Smart Card without changing any of the other details stored on the card.

The old PIN must be submitted before a change is effected and the new PIN must be supplied correctly at two consecutive prompts.

Inputs: Smart Card PIN: 4 to 8 alphanumeric characters

Outputs: Text messages:
Insert Card and press ENTER when ready.
Enter current PIN.
Enter new PIN.
Re-enter new PIN.
PIN REJECTED BY CARD.
NOT A LMK CARD OR CARD NOT FORMATTED.
NEW PINS DO NOT MATCH! PLEASE RE-ENTER.
PIN change completed.

Example:

Online> NP < Return >

Insert Card and press ENTER when ready: < Return >
Enter current PIN: * * * * * * * < Return >
Enter new PIN: * * * * * < Return >
Re-enter new PIN: * * * * * < Return >
NEW PINS DO NOT MATCH! PLEASE RE-ENTER
Enter new PIN: * * * * * < Return >
Re-enter new PIN: * * * * * < Return >
PIN change completed
Online>

17.5 Reading Unidentifiable Smart Card Details

Command: RC (can be used online and offline).

Function: To read otherwise unidentifiable cards and display the CD zone details.

Inputs: None.

Outputs: Text messages:
Insert Card and press ENTER when ready.
NOT AN LMK CARD OR CARD NOT FORMATTED.
Version, as stored on card: decimal integer.
Date, as stored on card; format: YY/MM/DD.
Time, as stored on card; format: hh:mm:ss.
User ID, as stored on card; free format alphanumeric.
Issuer ID, as stored on card; free format alphanumeric.
Data Zone Size, as stored on card: decimal integer.
Max Data Free, as stored on card: decimal integer.

Example:

Online> RC < Return >

Format version: 0001
Issue time: 11:53:00
Issue date: 93/10/25
User ID: Bill Weasel
Issuer ID: Big Bank plc
User-data zone size: 0000
Free: 0392

17.6 Copying a PROM to a Smart Card

Command: PC (Offline only).

Function: To copy the LMK values stored on an LMK PROM to a formatted LMK Smart Card.

Inputs: Smart Card PIN: 4 to 8 alphanumeric characters.

Outputs: Component Set check value: 16 hexadecimal characters.
Text messages:
Insert both Card and PROM device and press ENTER when ready.
NOT AN LMK CARD OR CARD NOT FORMATTED.
COPY FAILED, PROM BLANK.
PIN REJECT BY CARD.
CARD CONTAINS LMK SET, OVERWRITE? [Y/N].
COPY COMPLETE, CHECK = XXXX XXXX XXXX XXXX.
COPY FAILED.

Example:

Offline > PC < Return >

Insert both Card and PROM devices and press ENTER < Return >
Enter PIN: * * * * < Return >
Writing Keys ...
Checking Keys ...
Copy complete, check: 0123 4567 89AB CDEF
Offline >

18 VISA CASH SYSTEM

The HSM provides Console commands to support the VISA Cash application:

- Export a Master Load Key (*KML).
- Import a Master Load Key (*KML).

(Keys with * must be double-length).

Always use a double-length ZMK with the VISA Cash System unless operating considerations make this impractical. To implement this, set the ZMK length parameter in the CS command to D.

Note that this has an impact on all the ZMKs used with this particular HSM.

18.1 Generate and Export a Master Load Key (*KML)

Command: DA (can be used online and offline).

Function: To generate a double-length Master Load Key (*KML) and return it encrypted under Variant 2 of LMK pair 04-05, and under a Zone Control Master Key (ZCMK). A check value for the *KML is also returned.

Input: *ZCMK, encrypted under LMK pair 04-05: 32 hexadecimal characters.

(Optional) Atalla Variant – 1 or 2 numeric digit; this value is required only if support for Atalla variants is set using the “CS” Console command (see Ref.2)

Outputs: *KML, encrypted under the ZCMK: 32 hexadecimal characters.

*KML, encrypted under Variant 2 of LMK pair 04-05.

*KML check value, formed by encrypting a block of binary zeros with the key and returning the left-most 24 bits of the result: 6 hexadecimal characters.

Errors: INVALID. The entered value does not contain 32 hexadecimal characters. Re-enter the correct number of characters.

KEY PARITY ERROR. The plaintext key does not have odd parity on each byte. Re-enter the correct value.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example (including support for Atalla variants):

Online > DA < Return >

Enter ZCMK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
(Enter ZMK variant: V < Return >, if enabled by CS command).

*KML encrypted for transmission: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
*KML encrypted under LMK: YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY

Key Check Value: ZZZZZZ

18.2 Importing a Master Load Key (*KML)

Command: DB (can be used online and offline).

Function: To translate a double-length Master Load Key (*KML) from encryption under a Zone Master Key (*ZCMK) to encryption under Variant 2 of LMK pair 04-05. A check value for the *KML is also returned.

Inputs: *ZMK, encrypted under LMK pair 04-05: 32 hexadecimal characters.

(Optional) Atalla Variant – 1 or 2 numeric digit; this value is required only if support for Atalla variants is set using the "CS" Console command (see Ref.2,)

*KML, encrypted under the *ZMK: 32 hexadecimal characters.

Outputs: *KML, encrypted under Variant 2 of LMK pair 04-05.

*KML check value, formed by encrypting a block of binary zeros with the key and returning the left-most 24 bits of the result: 6 hexadecimal characters.

Errors: INVALID. The entered value does not contain 32 hexadecimal characters. Re-enter the correct number of characters.

KEY PARITY ERROR. The plaintext key does not have odd parity on each byte. Re-enter the correct value.

MASTER KEY PARITY ERROR. The contents of LMK storage have been corrupted or erased. Do not continue. Inform the Security Department.

Example:

Online > DB < Return >

Enter *ZCMK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
Enter *KML: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX < Return >
*KML encrypted under LMK: YYYY YYYY YYYY YYYY YYYY YYYY YYYY YYYY

Key Check Value: ZZZZ

19 AMERICAN EXPRESS CARD SECURING CODE

19.1 Generate a CSCK

Command: YA

Function: To generate a new *CSCK and display it encrypted under the LMK.

Inputs: A CSCK length flag.

Outputs: The new CSCK, encrypted under LMK 14-15 variant 4.

Errors: MASTER KEY PARITY ERROR - the contents of LMK storage have been corrupted or erased. Do not continue; inform the Security Department.

Example:

Online > YA

Enter CSCK length [S/D]: D

Encrypted *CSCK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Online > YA

Enter CSCK length [S/D]: S

Encrypted CSCK: XXXX XXXX XXXX XXXX

19.2 Export a CSCK

Command: YB

Function: This command will accept a Zone Master Key (ZMK) and a CSCK encrypted under the LMK. It will decrypt and check parity on both keys, and if correct will encrypt the CSCK under the ZMK and display it.

Inputs: A flag to indicate the length of the ZMK.

A ZMK encrypted under LMK 04-05 (generated by the “DE” command), 16/32 hexadecimal characters.

A ZMK variant (or <Return> to ignore). **Note:** the Atalla variant support parameter (set with the “CS” command) is ignored.

A CSCK encrypted under LMK 14-15 variant 4, 16/32 hexadecimal characters.

Outputs: The CSCK encrypted under the ZMK.

A Key Check Value (KCV) for the CSCK.

Errors: INVALID - the keys are not 16/32 hexadecimal digits in length.

KEY PARITY ERROR; RE-ENTER KEY: - the key just entered did not have odd parity; check for typographical errors and re-enter.

MASTER KEY PARITY ERROR - the contents of LMK storage have been corrupted or erased. Do not continue; inform the Security Department.

Example:

Online > YB

Enter ZMK length [S/D]: D
Enter *ZMK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
Enter *CSCK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

*CSCK encrypted for transmission: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Key check value: XXXXXX

Online > YB

Enter ZMK length [S/D]: S
Enter ZMK: XXXX XXXX XXXX XXXX
Enter CSCK: XXXX XXXX XXXX XXXX

CSCK encrypted for transmission: XXXX XXXX XXXX XXXX
Key check value: XXXXXX

19.3 Import a CSCK

Command: YC

Function: This command will accept a Zone Master Key (ZMK) encrypted under the LMK and a CSCK encrypted under the ZMK. It will decrypt and check parity on the ZMK, and if correct will use it to decrypt the CSCK. Incoming CSCK parity will be ignored, but will be forced odd before encryption under the LMK.

Inputs: A flag to indicate the length of the ZMK.

A ZMK encrypted under LMK 04-05 (generated by the “DE” command), 16/32 hexadecimal characters.

A ZMK variant (or <Return> to ignore). **Note:** the Atalla variant support parameter (set with the “CS” command) is ignored.

A CSCK encrypted under the ZMK, 16/32 hexadecimal characters.

Outputs: The CSCK encrypted under LMK 14-15 variant 4.

A Key Check Value (KCV) for the CSCK.

Errors: INVALID - the keys are not 16/32 hexadecimal digits in length.

KEY PARITY ERROR; RE-ENTER KEY: - the key just entered did not have odd parity; check for typographical errors and re-enter.

MASTER KEY PARITY ERROR - the contents of LMK storage have been corrupted or erased. Do not continue; inform the Security Department.

CSCK ALL-ZERO - The clear CSCK is all zeros, and will not be translated.

Example:

Online > YC

Enter ZMK length [S/D]: D
Enter *ZMK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX
Enter *CSCK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

*CSCK encrypted under LMK: XXXX XXXX XXXX XXXX XXXX XXXX XXXX XXXX

Key check value: XXXXXX

Online > YC

Enter ZMK length [S/D]: S
Enter ZMK: XXXX XXXX XXXX XXXX
Enter CSCK: XXXX XXXX XXXX XXXX

CSCK encrypted under LMK: XXXX XXXX XXXX XXXX
Key check value: XXXXXX

GLOSSARY

Authorised State
The HSM must be set into the Authorised state before certain 'privileged' functions can be performed. This can be achieved only by Authorising Officers using their Passwords/Smart Cards. The Authorized state is required for all operations that are more sensitive than normal, such as the entry of ZMK components and any other functions that involve clear (unencrypted secret data).

Card Account Number
Primary Account Number (PAN) as embossed on the plastic card.
Cardholder-Selected PIN
A PIN created by the cardholder. This provides an opportunity for the cardholder to create a PIN that can be easily remembered (instead of using an arbitrary combination of numbers allocated by the card issuer).

Component
A value which, when combined with other similar values, forms a key. The method of combination is the exclusive-OR function. For example, three Secret Values are components of an HSM Local Master Key or a Zone Master Key.

Derived PIN
A PIN that has been derived from a value associated with a particular cardholder. The value is usually the cardholder's account number.

DES Key
A secret 56-bit value (64 bits if 8 parity bits are included) that is an input to the DES algorithm. It controls the transformation of data during encryption/decryption.

Exclusive-OR
Modulo 2 addition, which is equivalent to binary addition without carry.

Key Separation
The ability to ensure that cryptographic keys defined for one purpose cannot be used illegally for another purpose.

LMKs (Local Master Keys)
The HSM resident DES keys that govern all HSM cryptographic functions. Used to encrypt all other DES keys, and to encrypt PINs that are to be stored by the Host in a database.

LMK Storage
The random access memory reserved for the storage of the HSM Master Keys. Data in this memory area is protected against power failure, and it is automatically erased when the HSM is opened.

Local Master Key Pair
One pair of the DES keys that reside in internal, battery-protected memory.

MAC (Message Authentication Code)
A cryptographic check value which is generated and verified to ensure that messages transmitted from one location and received at another have not changed in any way. The left-most 32 bits of the Message Authentication output Block (MAB).

MR (MAC Residue)
The right-most 32 bits of the Message Authentication output Block (MAB).

Natural PIN
A PIN that can be derived from the account number or other constant data. It can always be recreated, given the original PIN-creation parameters.

Not On Us
Financial transaction on an account not held by the recipient bank.

Offset (PIN)
The difference between a random or cardholder-selected PIN, and the natural PIN for that cardholder. Used to verify a cardholder's PIN entry. Can be stored in a file as an alternative to maintaining a file of encrypted PINs.

On Us
Financial transaction on an account held by the recipient bank.

OWF
One Way Function.

Password
A 16-character value or phrase, known only to an Authorizing Officer, and stored in the HSM. Two are used, and stored as Master Keys 00 and 01. Passwords are entered at the Console to set the HSM into the Authorized state. When the HSM is configured for Smart Card use, the Passwords are random values stored on the Smart Cards (and PINs replace the Passwords functionally).

PIN Block
A 64 bit value which is formed from a PIN and account number (normally). It is used in transmitting the PIN from one location to another (in encrypted form).

PIN Check Key
A DES key that controls the IBM method of PIN and offset generation.

PIN or Key Conveyance Mailer
A printed, multi-part form arranged such that it conceals the printed secret information (such as a cardholder PIN, or a key, or a key component). The mailer is constructed in such a way that the secret information (e.g.,, PIN and reference number) cannot be read unless the mailer is torn open. It can be mailed or otherwise carried to another network node, or stored in a (secure) conventional filing system.

PIN (Smart Card)
Alphanumeric Password used to allow access to data stored on a Smart Card.

PIN Solicitation Mailer
A special PIN mailer used by the cardholder to return a PIN selection to the issuer. The mailer is constructed in such a way that the secret information (e.g.,,, PIN and reference number) cannot be read unless the mailer is torn open. The return part of the mailer contains only the clear PIN and an encrypted reference to the Card Account Number.

PIN Verification Key (PVK)
A DES key that controls the generation and verification of PINs and offsets.

PIN Verification Key Indicator (PVKI)
A 1-digit value that is used to generate a PIN Verification Value. It is used in VISA ATM Networks to indicate which of six possible pairs of PIN Verification Keys is required to generate a PIN Verification Value.

PIN Verification Value (PVV)
A value that is derived from the account number, the PIN, a PIN Verification Key Indicator, and a pair of PIN Verification Keys. Used to verify a cardholder's PIN entry in VISA ATM Networks.

PROM
Programmable Read-Only Memory. Used to store the program logic (firmware). (Also used for storing components of the LMK in older HSMs (this allows re-installation of the LMK at a later date if required)).

Privileged Function
An HSM function that involves the presence of clear, unprotected keys or PINs. A function which presents a security risk unless adequate controls are established, and it requires the presence of the LMK Component Holders or the assertion of the Authorized state.

RSA Key
A pair of cryptographic variables (secret key and public key) used in a Rivest, Shamir and Adleman public key crypto system.

Reference Number
A number produced by the HSM by encrypting part of the cardholder account number under a pair of Local Master Keys. Used as a security measure in PIN solicitation procedures, to prevent an adversary from discovering the cardholder's PIN selection.

Solicitation-Only Mailer
A printed, multi-part, turnaround form sent to a cardholder for selecting a PIN. (See PIN Solicitation Mailer).

Source Key
The key used for encryption by the source of a transaction message (i.e.,, a terminal or Host computer).

Terminal
ATMs and similar electronic point-of-sale devices capable of a variety of cryptographic functions, e.g.,, PIN encryption, PIN verification and message authentication.

Terminal Authentication Key (TAK)
A terminal-resident DES key for creating a message authentication code on data in outgoing messages.

Termination Encryption Key (TEK)
A terminal resident DES key for encrypting data in outgoing messages.

Terminal Master Key (TMK)
A terminal-resident DES key for encrypting other keys. In some cases, the TMK is also used for PIN encryption and/or PIN verification.

Terminal PIN Key (TPK)
A terminal-resident DES key for encrypting PINs in outgoing messages, and/or for terminal PIN verification.

Three Tier Key Hierarchy
Contains Master Keys, Transport Keys and Data Keys. The Master Keys are manually distributed, the others are distributed electronically. Master Keys are normally available only in two or more components. Data keys are also known as Session Keys.

Translate, Translation
A decrypt-then-re-encrypt process which changes the key under which data is encrypted (e.g.,, translating a PIN from a Terminal PIN Key to a Zone PIN Key).

User Storage
The 12K random access memory reserved for the storage of user keys, the Diebold Proprietary Algorithm Table, and the processing of PIN solicitation data from the Host. This memory area is automatically erased when the HSM is opened or when power is removed.

Watchword, Watchword Key (WWK)
User verification key used in the Racal Watchword token or system.

Working Key (WK)
VISA name for a Zone PIN Key.

Zone Authentication Key (ZAK)
Used to create MACs on messages between institutions (i.e., in a defined cryptographic zone).

Zone Control Master Key (ZCMK)
VISA name for ZMK.

Zone Encryption Key (ZEK)
Used to encrypt data between institutions (i.e., in a defined cryptographic zone).

Zone Master Key (ZMK)
The master key used in a shared (interchange) network to protect other keys during conveyance. (Manually transported key encrypting key. Transported as three components and formed by combining the components using the exclusive-OR function).

ZMK Component
A 16-digit value. Three ZMK components are exclusive-OR combined to form a ZMK.

ZMK Variant (Atalla) Support
Provides support for ZMKs created in systems using Atalla security modules. The variant is a single digit value in the range 0-9, where:

Value	Key Encrypted by the ZMK
1	ZPK
2	ZEK
3	CVK and ZAK
4	PVK
5	ATM Key (≡TMK)
8	Derivation Key (DK)

Zone PIN Key (ZPK)
The data-encrypting key used to encrypt PINs for transmission over a shared (interchange) network.

Zone Transport Key (ZTK)
Used to encrypt zone session keys (i.e., ZEK, ZAK, etc.) for electronic delivery. Similar to ZMK.

General Abbreviations

ATM	:	Automated Teller Machine.
AWK	:	Acquirer Working Key.
CVK	:	Card Verification Key.
CVV	:	Card Verification Value.
DCE	:	Data Communications Equipment.
DES	:	Data Encryption Standard.
DTE	:	Data Terminal Equipment.
EFTPOS	:	Electronic Funds Transfer at Point of Sale.
IWK	:	Issuer Working Key.
KCV	:	Key Check Value.
LMK	:	Local Master Key.
MAC	:	Message Authentication Code.
PAN	:	Primary Account Number.
PIN	:	Personal Identification Number.
PROM	:	Programmable Read-Only Memory.
PVK	:	PIN Verification Key.
PVKI	:	PIN Verification Key Indicator.
PVV	:	PIN Verification Value.
RAM	:	Random Access Memory.
RSA	:	Rivest, Shamir and Adleman public key scheme.
TAK	:	Terminal Authentication Key.
TDK	:	Terminal Derivation Key.
TCP	:	Transport Control Protocol.
TEK	:	Terminal Encryption Key.
TMK	:	Terminal Master Key.
TPK	:	Terminal PIN Key.
X'NN	:	A 2-digit hexadecimal value, often used to represent a 1-byte value.
ZMK	:	Zone Master Key.
ZPK	:	Zone PIN Key.
ZTK	:	Zone Transport Key.
WK	:	Working Key.
WWK	:	Watchword Key.
ZAK	:	Zone Authentication Key.
ZCMK	:	Zone Control Master Key.
ZEK	:	Zone Encryption Key.

SNA-SDLC Abbreviations

AID	Attention Identifier.
BB,EB	Begin Bracket, End Bracket. SNA Brackets are used to delimit transactions. In the HSM environment they can be used to carry-out a change of direction (CD) on the link. Bracketing is only of limited use with HSMs.
BC,EC	Beginning of Chain and End of Chain Bits: 00 : Middle in Chain : MIC. 01 : End of Chain : LIC. 10 : Beginning of Chain : FIC. 11 : Only in Chain : OIC.
BETB	3274 "Between Bracket" State. After EB and before BB (i.e.,]..here..[ ).
CD	Change Direction so that the other LU has control.
CSI	Bit in RH defining "Code Selection Indicator".
DFC	Data Flow Control command. SNA command to control the flow of data in LU-LU sessions.
FIC	First in Chain. Position of a request (RU) in an SNA Chain.
FMD	Function Management Data command. SNA Command for Data transfer between LUs (LU-LU).
INB	3274 "In Bracket" State. After BB and before EB (i.e., [..here..]).
IPR	Isolated Pacing Response.
LIC	Last in Chain. Position of a request (RU) in an SNA Chain.
LU	SNA Logical Unit, entity which partakes in SNA sessions.
MIC	Middle in Chain. Position of a request (RU) in an SNA Chain.
OIC	Only in Chain.
PEND.B	3274 "Pending Begin Bracket" State.
B	A 3270 Terminal user has started to type but has not yet pressed <Enter>.
PLU	SNA Primary Logical Unit; normally the application program in the Host computer.
PU	SNA Physical Unit, can contain several LUs (e.g.,, a 3274 Cluster Controller).
RCV	Receive state.
RH	Request/Response Header (3 bytes).
RQD	Definite Request/Response. The recipient must reply to this message.
RQE	Exception Request/Response. The sender does not expect a reply unless there is a problem.
+RSP	A positive (affirmative) response to an SNA request.
RU	Request/Response Unit.
SBA	Set Buffer Address.
SDT	Start Data Traffic.
SLU	SNA Secondary Logical Unit; normally a terminal or the HSM.
SSCP	SNA System Services Control Point; normally resides in the Communications Controller (37x5) and responsible for controlling access to the PU and SLU.
TH	Transmission Header (6 bytes).
WCC	Write Control Character (3270).
WSF	Write Structured Field.
X'NNNN	A 4-digit hexadecimal value.

Appendix A
Bisynchronous Connected Option, Programming Examples

1 GENERAL

This Appendix shows examples of IBM system configuration data used in bisynchronous environments.

2 EXAMPLES

A. Sample 1:VTAM/NCP-

LINE721	LINE	ADDRESS=33,	LINE ADDRESS
		SPEED=96000,	LINE SPEED
		CLOCKNG=EXT,	MODEM CLOCKING USED
		DUPLEX=FULL,	FULL DUPLEX MODE
		DATRATE=HIGH,	REQ.
		NEWSYNC=NO,	NO NEWSYNC FEATURE
		POLLED=YES,	LINE IS POLLED
		POLIMIT=(1 QUEUE),	
		RETRIES=10,	ERROR REC. ATTEMPTS
		SERVLIM=2,	SERVIC ORDER TABLE SCANS
		SESSION=4,	SESSION COUNT FOR LINE
		OWNER=SSCPA,	3083B
		ISTATUS=ACTIVE	INITIAL STATUS
	SERVICE ORDER=(VS21P1A, VS211A00, VS21P1B, VS211B00)		
VS21P1A	CLUSTER	CUTYPE=3271,	
		GPOLL=40407F7F,	
		TERM=3277, ISTATUS=ACTIVE	
VS211A00	TERMINAL	ADDRESS=60604040,	
		POLL=40404040, ISTATUS=ACTIVE, LOGAPPL=CICS2	
VS21P1B	CLUSTER	CUTYPE=3271,	
		GPOLL=C1C17F7F,	
		TERM=3277, ISTATUS=ACTIVE	
VS211A00	TERMINAL	ADDRESS=61614040,	
		POLL=C1C14040, ISTATUS=ACTIVE	
LINE722	LINE	ADDRESS=34,	LINE ADDRESS
		SPEED=96000,	LINE SPEED
		CLOCKNG=EXT,	MODEM CLOCKING USED
		DUPLEX=FULL,	FULL DUPLEX MODE
		DATRATE=HIGH,	REQ.
		NEWSYNC=NO,	NO NEWSYNC FEATURE
		POLLED=YES,	LINE IS POLLED

```
                                POLIMIT=(1 QUEUE),
                                RETRIES=10,             ERROR REC.ATTEMPTS
                                SERVLIM=2,              SERVIC ORDER TABLE
                                                        SCANS
                                SESSION=2,              SESSION COUNT FOR LINE
                                OWNER=SSCPA,            3083B
                                ISTATUS=ACTIVE          INITIAL STATUS

                SERVICE ORDER=(VS21P1A, VS211A00)
VS22P1A         CLUSTER         CUTYPE=3271,
                                GPOLL=40407F7F,
                                TERM=3277, ISTATUS=ACTIVE

VS211A00        TERMINAL        ADDRESS=60604040,
                                POLL=40404040, ISTATUS=ACTIVE, LOGAPPL=CICS2
```

B. SAMPLE 2: (NCP VERSION 4.2 ON AN IBM 3270)

```
*                               BSC LEASED LINE GROUP                   *

LG03BSC1        GROUP           ATTACH=MODEM,           MODEM ATTACHED
                                CLOCKNG=EXT,            EXTERNAL MODEM CLOCKING
                                CODE=EBCDIC,
                                CUTOFF=1,
                                DIAL=NO,                NON-SWITCHED LINES
                                DUPLEX=FULL,            FULL DUPLEX CONNECTION
                                FEATURE=GPLKUP,         LOOKUP DEVICE
                                INHIBIT=SUBBLOCK,       RECOMMENDED
                                LNCTL=BSC,              LINE CONTROL IS BSC !!
                                NEGPOLP=0.2,            NEGATIVE POLLING PAUSE
                                NEWSYNC=NO,             NO NEWSYNC CHARS
                                PAUSE=1,                PAUSE BETWEEN SRVC
                                                        CYCLES
                                POLLED=YES,             BSC DEVICES TO BE POLLED
                                RETRIES=(7,4,5),        RETRY SEQUENCE
                                TYPE=NCP,
                                TRANSFR=3

*                       LINE L103FC (BSC) --  HOST SECURITY MODULE      *
L103FC          LINE            ADDRESS=(3,HALF),       3270 ADDRESS
                                SPEED=9600              DOCUMENTATION (AND FOR
                                                        NPM)
*
                SERVICE ORDER=(PUFC1.LUFC1S00.PUFC2,LUFCIS01.PUFC3,LUFC1S02)
PUFC1           CLUSTER         CUTYPE=3271,            SEEN AS A 3271
                                GPOLL=40407F7F,         GENERAL POLL ADDRESS
                                ISTATUS=ACTIVE          DEFAULT STATUS IS INACTIVE
*
LUFC1S00        TERMINAL        TERM=3277,              SEEN AS A 3277
                                ADDRESS=60604040,       SELECTION ADDRESS
```

```
                                POLL=40404040           POLL ADDRESS
*
PUFC2           CLUSTER         CUTYPE=3271,            SEEN AS A 3271
                                GPOLL=C1C17F7F,         GENERAL POLL ADDRESS
                                ISTATUS=ACTIVE          DEFAULT STATUS IS INACTIVE
*
LUFC1S01        TERMINAL        TERM=3277,              SEEN AS A 3277
                                ADDRESS=61614040,       SELECTION ADDRESS
                                POLL=C1C14040           POLL ADDRESS
*
PUFC3           CLUSTER         CUTYPE=3271,            SEEN AS A 3271
                                GPOLL=C2C27F7F,         GENERAL POLL ADDRESS
                                ISTATUS=ACTIVE          DEFAULT STATUS IS INACTIVE
*
LUFC1S02        TERMINAL        TERM=3277,              SEEN AS A 3277
                                ADDRESS=E2E24040,       SELECTION ADDRESS
                                POLL=C2C24040           POLL ADDRESS
```

C) CICS DFHTCT (Terminal Control Table)

```
* HOST SECURITY MODULES

HSM1            DFHTCT          TYPE=TERMINAL,TRMTYPE=3277,TRMMODL=1,TRMIDNT=HSM1,ACCMETH
                                =VTAM,
                                RELREQ=(YES,YES),TRMSTAT=TRANSCEIVE,GMMSG=NO,TIOAL=2000,
                                FEATURE=(UCTRAN,DCKYBD),TRANSID=VB50,NETNAME=VS21IB00,CONNE
                                CT=AUTO

HSM2            DFHTCT          TYPE=TERMINAL,TRMTYPE=3277,TRMMODL=1,TRMIDNT=HSM2,ACCMETH
                                =VTAM,
                                RELREQ=(YES,YES),TRMSTAT=TRANSCEIVE,GMMSG=NO,TIOAL=2000,
                                FEATURE=(UCTRAN,DCKYBD),TRANSID=VB50,NETNAME=VS21IA00,CONNE
                                CT=AUTO

HSM3            DFHTCT          TYPE=TERMINAL,TRMTYPE=3277,TRMMODL=1,TRMIDNT=HSM3,ACCMETH
                                =VTAM,
                                RELREQ=(YES,YES),TRMSTAT=TRANSCEIVE,GMMSG=NO,TIOAL=2000,
                                FEATURE=(UCTRAN,DCKYBD),TRANSID=VB50,NETNAME=VS21A00,CONNE
                                CT=AUTO
```

Note: The aforementioned NETNAMES refer to Sample A

D) CICS DFHDCT (Destination Control Table)

Note: There must be an entry like the following for each HSM* in the network matching the ‘trmidnt=' option of the tct

* Host Security Modules

```
HSM1    DFHTCT    TYPE=INTRA,DESTID=HSM1,TRIGLEV=1,TRANSID=VB40,DESTFAC=TER
                  MINAL

HSM2    DFHTCT    TYPE=INTRA,DESTID=HSM2,TRIGLEV=1,TRANSID=VB40,DESTFAC=TER
                  MINAL

HSM3    DFHTCT    TYPE=INTRA,DESTID=HSM3,TRIGLEV=1,TRANSID=VB40,DESTFAC=TER
                  MINAL
```

IBM 937X CICS and VTAM Configuration Example

The values of certain parameters may be chosen by the user installing the HSMs, these are marked “User defined”.

CICS Terminal Control Table

```
*   ICA     CONTROLLED REMOTE TERMINAL ENTRIES                          *

HSM1        DFHTCT TYPE=TERMINAL,                                       X
                        ACCMETH=VTAM,                                   X
                        FEATURE=(UCTRAN,DCKYBD),                        X
                        CONNECT=AUTO,                                   X
                        GMMSG=NO,                                       X
                        NETNAME=VIHSMO1,                                X User Defined
                        RELREQ(YES,YES),                                X
                        TIOAL=2000,                                     X
                        TRMIDNT=HSM1,                                   X User Defined
                        TRMMODL=1,                                      X
                        TRMSTAT=TRANSCEIVE,                             X
                        TRANSID=VB50,                                   X User Defined
                        TRMTYPE=3277

HSM2        DFHTCT TYPE=TERMINAL,                                       X
                        ACCMETH=VTAM,                                   X
                        FEATURE=(UCTRAN,DCKYBD),                        X
                        CONNECT=AUTO,                                   X
                        GMMSG=NO,                                       X
                        NETNAME=VIHSMO2,                                X User Defined
                        RELREQ(YES,YES),                                X
                        TIOAL=2000,                                     X
                        TRMIDNT=HSM2,                                   X User Defined
                        TRMMODL=1,                                      X
                        TRMSTAT=TRANSCEIVE,                             X
                        TRANSID=VB50,                                   X User Defined
                        TRMTYPE=3277,
```

Note that "the transaction ID "VB50" is that defined by the resident HSM interface software.

VTAM Group and Line Macros

```
VIBSB823    VBUILD TYPE=CA
*
VIBSCGR1    GROUP LNCTL-BSC
*LINE B82   (PORT 21-1 ON ICA)
LB82        LINE ADDRESS=B82,ISTATUS=ACTIVE
VICLUS82    CLUSTER GPOLL=40,              X
            CUTYPE=3271,ISTATUS=ACTIVE
VIHSMO1     TERMINAL ADDR=40,              X
            TERM=3277                      X
            DLOGMOD=D4C32771               X
            ISTATUS=ACTIVE,                X
            FEATUR2=(MODEL1)
*
* LINE B83 (PORT 21-2 ON ICA)
LB83        LINE ADDRESS=B83,INSTATUS=ACTIVE
VICLUS83    CLUSTER GPOLL=40,              X
            CUTYPE=3271,ISTATUS=ACTIVE
VIHSM02     TERMINAL ADDR=40,              X
            TERM=3277,                     X
            DLOGMOD=D4C32771,              X
            ISTATUS=ACTIVE,                X
            FEATUR2=(MODEL1)
```

Note that all group, cluster and terminal names may be user defined.

From the "Top Level" screen:
for hardware config.

QFJB82

Clocking	1 (DCE)
Line speed	9600
Switched Line	N
Select Standby	N
Modem Protocol	O (DTR)
Permanent Request to Send	Y
Line Code	O (EBCDIC)
Include Header	O (No)
Data Rate Select	O (Full)
Line Utilization Buffer Length	24
Line Utilization Threshold	60
Tributary Address	4060

This is repeated for line "B83".

Appendix B
Asynchronous Connected Option, Programming Examples

1 GENERAL

This Appendix shows examples of IBM system configuration data for AS400 when connecting an HSM via asynchronous means.

2 EXAMPLE

```
Line Description                          LIND        L091SMDC
Option                                    OPTION      *ALL
Category of line                                      *ASYNC

Resource Name                             RSRCNAME    LIN091
Online at IPL                             ONLINE      *YES
Physical interface                        INTERFACE   *RS232V24
Connection type                           CNN         *NONSWTPP
Switched network backup                   SNBU        *NO
Modem type supported                      MODEM       *NORMAL
Modem data rate select                    MODEMRATE   *FULL
Autoanswer type                           AUTOANSTYP  *DTR
Error threshold level                     THRESHOLD   *OFF
Text                                      TEXT        *BLANK

Attached nonswitched controllers          CTL

---------Attached Nonswitched controllers---------------------

C091SMDC

End-of-Record table                       EORTBL

---End-of-record Table---                 ---End-of-record Table---
End-of-record   Trailing                  End-of-record     Trailing
 Characters    Characters                   Characters      Characters

    00             0                          00             0
    00             0                          00             0
    00             0                          00             0
    00             0                          00             0

Data bits per character                   BITSCHAR    7
Type of parity                            PARITY      *EVEN
Stop bits                                 STOPBITS    1
Duplex                                    DUPLEX      *FULL
Echo support                              ECHO        *NONE
Line speed                                LINESPEED   9600
Maximum buffer size                       MAXBUFFER   1024
Flow control                              FLOWCNTL    *NO

Idle timer                                IDLTMR      1
Data Set Ready drop timer                 DSRDRPTMR   6
Clear To Send timer                       CTSTMR      25
Remote answer timer                       RMTANSTMR   50
Recovery limits                           CMNRCYKLMT
    Count limit                                       2
    Time interval                                     5
```

```
Controller description                  CTLD        C091SMDC
Option                                  OPTION      *ALL
Category of controller                              *ASC

Link type                               LINKTYPE    *ASYNC
Online at IPL                           ONLINE      *YES
Switched connection                     SWITCHED    *NO
Switched network backup                 SNBU        *NO
Attached nonswitched line               LINE        L091SMDC
Remote verify                           RMYVFY      *NO
Text                                    TEXT        *BLANK

Attached devices                        DEV
---------------------Attached Devices-----------------------

D091SMDC

File transfer ack timer                 ACKTMR      16
File transfer retry                     RETRY       7
Recovery limits                         CMNRCYKLMT
    Count limit                                     2
    Time interval                                   5


Device description                      DEVD        D091SMDC
Option                                  OPTION      *ALL
Category of device                                  *ASYNC

Remote location                         RMTLOCNAME  D091SMDC
Online at IPL                           ONLINE      *NO
Attached controller                     CTL         C091SMDC
Text                                    TEXT        *BLANK
```

Appendix C
Channel Attach Option, Configuring the Mainframe

1 GENERAL

The sequence below is an example of how to define the HSM to the mainframe using the Hardware Confirmation Definition (HCD). The sequence may be slightly different in a particular environment. The Hardware Configuration Definition program can be accessed from TSO under MVS. Refer to the IBM Manuals:

Hardware Configuration Definition: Users Guide IBM MVS/ESA - GC33-6457
System commands - GC28-1626

ES/9000: Operating Your System - SA24-4350 (Or the equivalent for the particular mainframe).

2 SEQUENCE

From the main HCD panel select option 4 - Define Control Unit Data:

Press <Enter>.
Press <F11> to Add.

In the "Add Control Unit" panel specify:

Control Unit Number	<As chosen for the particular environment>
Control Unit Type	DUMMY
Description	HSM (Dummy) Control Unit

Press <Enter>.

In the "Select Processor/Control Unit" panel, enter C against the relevant processor ID to change it:

Press <Enter> to display the "Add Control Unit" panel, and specify the chosen channel path ID (CHPID) and unit address.
Press <Enter>.
Press <Enter>.
Press <F12> to leave the "Control Unit List" panel.

At the main HCD panel, select option 5 to Define I/O device data:

Press <Enter>.
Press <F11> to display the "Add Device" panel:

Device Number	<Subchannel address of HSM device>
Device Type	DUMMY
Description	HSM (Dummy) Device
Connected to C.U.s	<Subchannel number of HSM Control Unit defined earlier>

Press <Enter> to display the "Device/Processor Definition" panel, and enter C against the relevant processor ID to change it.

Press <Enter> to display the "Define Device/Processor" panel.

Leave unit address unchanged.

Change Timeout to NO:

Press <Enter> to return to the "Device/Processor Definition" panel.

Press <Enter> to display the "Define Device to Operating System" panel, and enter C against the relevant processor ID to change it.

Press <Enter> to bring up the "Define Device Parameter/Features" panel.

Choose OFFLINE Yes/No to suit the particular requirements.

Change DYNAMIC to NO.

Press <Enter> to display the "List of EDT" panel.

Enter C against the relevant processor ID to change it.

Press <Enter> to display the "Assign Device to Esoteric" panel.

If required, add the HSM to the list of Esoteric devices.

Press <Enter> to return to the "List of EDTs" panel.

Press <Enter> to return to the "Define Devices to Operating System Configuration" panel.

Press <Enter> to show the "I/O Device List" (which should now include the new device).

Press <F12> to return to the main HCD panel.

3 ACTIVATING THE CHANGES

Having defined the HSM to the HCD, use option 6 from the HCD main menu to create an IO Configuration Dataset (IOCDS) that is accessible from the processor console.

Select option 6 to Activate configuration data:

Press <Enter>.
Select option 1 to Build production IO Definition file.
Press <Enter>.
Specify the name of the IODF and the DISK it is to reside upon. Note that the address of this disk must be specified in the load parameter of the Activation profile on the processor console.
Press <Enter>.

When the IODF has been created use option 2 to create the IOCDS (which is to reside on the processor console).

Select option 2 to Build IOCDS:

The submitted job creates the new IOCDS. It requests permission to update the IOCDS on the processor console. For this to occur, sign-on to the processor console and disable the write protect on the IOCDS that is to be updated.

Activate (or re-activate) (IML) MVS with an activation profile that picks up the new IOCDS. The 'Load Parameter' in the activation profile is used to point to the new IOCDS.

4 TEST PROGRAM

A test program, which can be used to send test transactions to an HSM channel-attached device, can be obtained from the local HSM service provider. It repeats commands and groups of commands a thousand times. The commands are determined by the first byte of the 'Param Parameter' when the program is initiated, as follows:

1 - 1 RA (revoke authorization commands)
2 - 7 Translate PIN block TPK to ZPK (various source and destination keys)
3 - 2 Verify PIN from Terminal using VISA PVV:
4 - 1 Generate a MAK using a TAK (over 128 byte message)
5 - 1 Generate a MAK using a TAK (over 127 byte message)
6 - 1 Generate a MAK using a TAK (over 129 byte message)
7 - 1 Generate a MAK using a TAK (over 256 byte message)
8 - 1 Generate a MAK using a TAK (over 512 byte message).

Appendix D
SNA-SDLC Connected Option, Programming Examples

1 GENERAL

This appendix provides a sample Network Control Program (NCP) “Gen” to define an HSM to the network.

2 HOST NCP CONFIGURATION

The parameters on the "Gen" statement are categorized as follows:

Required:	The HSM requires that these parameters are defined as in the sample.
Recommended:	It is recommended that these parameters are set as in the sample to achieve optimum performance from the HSM.
User Defined:	The HSM has no requirements with respect to these parameters.

All other parameters not listed in the sample "Gen" are left to their default values. Because it is not possible to test all possible configurations of IBM software and hardware, all of the parameters are subject to possible change in other environments.

3 CICS TCT

The sample CICS Terminal Control Table (TCT) definition parameters are marked as either "Required" or "User Defined".

4 VTAM BIND

This is the Bind that the HSM expects to see. The Bind should be used as given. Changing the Bind parameters may produce unpredictable results. For information on the meaning of the Bind parameters, refer to the VTAM customisation manual for the particular version of VTAM that is in use.

5 SAMPLE NCP AND HOST CONFIGURATION DATA

The data was compiled using the following IBM Hardware and Software:

Hardware: 3081, 3705 (also applies to 3725).
Software: MVS/XA 2.2, VTAM 3.2, CICS 1.7, NCP 3.1.

THIS IS A SAMPLE GEN TO DEFINE A RG7600 HSM TO A 37X5. THE 7600 EMULATES A 3274 MOD1A TERMINAL SNA TERMINAL CONTROLLER WITH A SINGLE TERMINAL ATTACHED.

```
 NCP DEFINITION FOR SNA/SDLC HSM (RG7500 or RG7600)
============================================================

*-------------------------------------------------------------------*
*  LINE L000
*  HSM
*-------------------------------------------------------------------*
L000     LINE  ADDRESS=(00,FULL),  LINE ADDRESS                      X
               ANS=CONTINUE,       CONTINUE LINK SERVICE            X
               CLOCKNG=EXT,        MODEM/EXT SOURCE PROVIDES CLOCKING  X
               DUPLEX=FULL,        REQUEST TO SEND ALWAYS UP        X
               ETRATIO=30,         ERROR-TO-TRANSMISSION-RATIO=3%   X
               IRETRY=NO,          NOT TO REPOLL SECONDARY STATION  X
               MODULO=8,           MAX NO. OF I-FRAME SENT BEFORE RESP X
               NRZI=NO,            NOT-RETURN-TO-ZERO-INVERTED      X
               PAUSE=(0.2,2.8),    POLLING CYCLE TIME               X
               SERVLIM=10,         10 SOT SCANS BEFORE SPECIAL SCAN X
               SPEED=9600,         EXTERNAL SOURCE CLOCKING RATE    X
               SRT=(,64),          SEND RECMS AFTER 64 ERRORS       X
               TYPE=NCP,           NETWORK CONTROL MODE             X
               ISTATUS=ACTIVE      (V) VTAM
*-------------------------------------------------------------------*
*  PU 4 FOR LINE L000 (FOR HSM)
*-------------------------------------------------------------------*
P000C4   PU    ADDR=C4,            PHYSICAL UNIT ADDRESS            X
               ANS=CONTINUE,       DON'T BREAK THE X-DOMAIN SESSIONS  X
               AVGPB=265,          AVERAGE POLL BUFFER              X
               MAXDATA=265,        MAXIMUM AMOUNT OF DATA           X
               MAXOUT=7,           MAX SDLC FRAMES BEFORE RESPONSE  X
               PACING=0,           PACING SET BY BIND IMAGE         X
               PASSLIM=7,          UP TO 8 PIU'S SENT TO PU AT 1 TIME  X
               PUDR=NO,            NO DYNAMIC RECONFIGURATION       X
               PUTYPE=2,           PU TYPE 2                        X
               RETRIES=(,2,1),     RETRY PAUSE 2 SECONDS FOR 1 TIMES  X
               SRT=(32000,100),    SYSTEM RECOVERY THRESHHOLD       X
               DISCNT=(NO),        (V) VTAM                         X
               ISTATUS=ACTIVE,     (V) VTAM                         X
               SSCPFM=FSS,         (V) VTAM                         X
               USSTAB=RACALUSS,    (V) VTAM                         X
               MODETAB=T4MODES3,   (V) VTAM                         X
               DLOGMOD=HSMBIND,    (V) VTAM                         X
               VPACING=0           (V) VTAM
*-------------------------------------------------------------------*
*        LU STATEMENTS FOR HSM
*-------------------------------------------------------------------*
T000C402 LU    LOCADDR=2
```

```
VTAM MODE TABLE
===============

         PRINT   NOGEN
RACALMOD MODETAB
  TITLE 'RACAL/HSM MODE TABLE '
*****************************************************************
*                                                               *
*  HOST SECURITY MODULE BIND IMAGE                              *
*                                                               *
*****************************************************************
RACALMOD MODEENT LOGMODE=RACALMOD,                                    X
               ENCR=X'00',                                            X
               TYPE=X'01',                                            X
               FMPROF=X'03',                                          X
               TSPROF=X'03',                                          X
               PRIPROT=X'B1',                                         X
               SECPROT=X'90',                                         X
               COMPROT=X'3080',                                       X
               RUSIZES=X'8787',                                       X
               PSNDPAC=X'00',                                         X
               SRCVPAC=X'00',                                         X
               SSNDPAC=X'00',                                         X
               PSNDPAC=X'00',                                         X
               SRCVPAC=X'00',                                         X
               SSNDPAC=X'00',                                         X
               PSERVIC=X'000000000000000000000000'
HSMBIND  MODEENT LOGMODE=HSMBIND,                                     X
               ENCR=X'00',                                            X
               TYPE=X'01',                                            X
               FMPROF=X'03',                                          X
               TSPROF=X'03',                                          X
               PRIPROT=X'B1',                                         X
               SECPROT=X'90',                                         X
               COMPROT=X'3080',                                       X
               RUSIZES=X'8787',                                       X
               PSNDPAC=X'00',                                         X
               SRCVPAC=X'00',                                         X
               SSNDPAC=X'00',                                         X
               PSERVIC=X'000000000000000000000000'
         MODEEND
         END



VTAM USSTAB
===========

         PRINT   NOGEN
RACALTAB USSTAB  FORMAT=DYNAMIC
LOGON    USSCMD  CMD=LOGON,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
LOGIN    USSCMD  CMD=LOGIN,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSP
*
SIGNON   USSCMD  CMD=SIGNON,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
```

```
SIGNIN   USSCMD  CMD=SIGNIN,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
*
SIGNIN   USSCMD  CMD=SIGNIN,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
TSO      USSCMD  CMD=TSO,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
HELLO    USSC     MD  CMD=HELLO,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
ALOHA    USSCMD  CMD=ALOHA,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
LOGOFF   USSCMD  CMD=LOGOFF,REP=LOGOFF,FORMAT=BAL
         USSPARM PARM=TYPE,DEFAULT=UNCOND
         USSPARM PARM=HOLD,DEFAULT=YES
         USSPARM PARM=APPLID,REP=APPLID
*
MESSAGES USSMSG  MSG=0,SUPP=ALWAYS
         USSMSG  MSG=1,SUPP=ALWAYS
         USSMSG  MSG=2,SUPP=ALWAYS
         USSM
         USSMSG  MSG=4,SUPP=ALWAYS
         USSMSG  MSG=5,SUPP=ALWAYS
         USSMSG  MSG=6,SUPP=ALWAYS
         USSMSG  MSG=7,SUPP=ALWAYS
         USSMSG  MSG=8,SUPP=ALWAYS
         USSMSG  MSG=9,SUPP=ALWAYS
         USSMSG  MSG=10,SUPP=ALWAYS
         USSMSG  MSG=11,SUPP=ALWAYS
         USSMSG  MSG=12,SUPP=ALWAYS
         USSMSG  MSG=9,SUPP=ALWAYS
         USSMSG  MSG=10,SUPP=ALWAYS
         USSMSG  MSG=11,SUPP=ALWAYS
         USSMSG  MSG=12,SUPP=ALWAYS
END      USSEND
         END
```

Appendix E
Standard Visa CW Test Data

1 GENERAL

This appendix shows the standard VISA CVV test data.

1.1 VISA Test Data

Account Number (PAN) 13 Digit	Expiry Date	Service Code	CVV
4123 456 789 012	8701	101	370
4999 988 887 777	9105	111	649
4666 655 554 444	9206	120	821
4333 322 221 111	9307	141	697

Account Number (PAN) 16 Digit	Expiry Date	Service Code	CVV
4123 4567 8901 2345	8701	101	561
4999 9888 8777 7000	9105	111	245
4666 6555 5444 4111	9206	120	664
4333 3222 2111 1222	9307	141	382

Plain text keys (CVKs):

Key A: 0123 4567 89AB CDEF
Key B: FEDC BA98 7654 3210

1.1 Test Data Converted for Use with HSM

The above CVK values when encrypted under the standard Test Local Master Key (LMK) set provided with each HSM are as follows:

Key A (CVKA): 0A61 E674 E88C 6A7E. Key Check Value (KCVA): D5D44F
Key B (CVKB): EABC 38C2 B2BB 492F. Key Check Value (KCVB): A68CDC

The values can then be used to test:

- The CW Host command (Generate a CVV).
- The CY Host command (Verify a CVV).
- Also, with a suitable ZMK, they can test the commands that translate CVKs between ZMK and LMK:
- The KB and KC Console commands.
- The AU and AW Host commands.

Appendix F
Warnings, Cautions and Statutory Statements

These Warnings, Cautions and Statutory Statements should be read before using the RG7000.

WARNINGS

Warnings are concerned with danger to personnel.

HIGH VOLTAGES

Always remove the power cable from the HSM power input connector before attempting to open the unit for maintenance purposes (for example to change a fuse).

Note however that if the local master keys (LMKs) are to be loaded from PROMs (and not Smart Cards), access is necessary to the inside of the unit while power is applied. Therefore observe the safety warnings displayed inside the unit. Avoid unnecessary contact with circuits inside the unit, and remove any metallic jewelry, such as watch straps and necklaces which might come into contact with circuits.

DANGEROUS SUBSTANCES

Semiconductor devices contain dangerous substances, such as beryllium and arsenic. Electronic devices must not be opened. If they become damaged, they must only be handled using protective gloves. If the substances inside electronic devices come into contact with broken skin or wounds, hospital care must be sought immediately. Electronic components must be disposed of as hazardous toxic waste and must not be incinerated.

GENERAL

At all times working practices must be in accordance with the health and safety at work act, and the control of substances hazardous to health (COSHH) regulations.

CAUTIONS

Cautions are concerned with damage to equipment or systems.

CMOS DEVICES

The electronic components in this unit use Complementary Metal Oxide Semiconductor (CMOS) techniques. All modules and components must be handled in accordance with the British Standards Institute BS 5783, the code of practice for Handling Static Sensitive Devices.

If the Local Master Keys (LMKs) are to be loaded from PROMs (and not Smart Cards), observe CMOS precautions while inserting and removing the PROM in the Zero Insertion Force (ZIF) socket: wear a standard electro-static discharge (ESD) wrist strap connected to the metal chassis of the HSM, or if a wrist strap is not available, touch the metal chassis of the HSM prior to touching the ZIF socket.

MAINS VOLTAGE SELECTION

The HSM requires either a 115 V or 230 V a.c. line supply. Before connecting, ensure that the correct mains voltage is selected (Chapter 2).

SAFETY STATEMENT

All Zaxus supplied products and systems are designed to meet their Technical Specifications and to ensure that they present no Health and Safety Hazards to the users.

It is the customer's obligation to install and operate these Products and Systems in the correct manner.

Some components in this Product contain substances that are subject to the Control of Substances Hazardous to Health Regulations, 1988 (COSHH). However, they present no hazard to the user when the product is used for the purpose for which it was designed, and in the manner indicated in the Manual.

If further information is required, contact your local Zaxus Sales Representative.

STATUTORY WARNINGS

This unit contains components which under certain circumstances could be considered potentially hazardous under the COSHH regulations of 1988.

If the equipment is used under its normal operating conditions there is no hazard to health.

Normal operating conditions are deemed to be those contained in this document.
If further information is required, contact your local Zaxus Sales Representative.

DECLARATIONS

Conformity To EU Directives

All the RG7000 series HSMs conform to the following EU Directives:

73/23/EEC the Low Voltage Directive.
89/336/EEC the EMC Directive.

Conformity to International Standards

The RG7000 series HSMs have been tested and meet or exceed the requirements of the following EMC Standards (See Note (1)):

EN55022 Class B.

EN50082-1:1992.
FCC Part 15, Class A (See Note (2)).

The RG7000 series HSMs have been tested and meet or exceed the requirements of the following Safety Standards:

EN60950
UL 1950

Notes:

When connecting to the RG7600 HSM installers are advised that the shield of the V.35 cable must be connected to the equipment chassis to ensure compliance with the requirements of EN55022 Class B and FCC Part 15 Class A.

Statement required under FCC rules: This equipment has been tested and found to comply with the limits for a Class "A" computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment

is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference in which case the user will be required to correct the interference at his own expense.

Other Declarations

Declaration under EU Directive 91/263/EEC, Article 2, covering Telecommunications Terminal Equipment:

The manufacturer/supplier: Zaxus, declares that: the RG7000 series of Host Security Module equipment is not intended to be connected to a public telecommunications network.

In respect of the European Union:

The connection of such equipment to a public telecommunications network in the Community Member State will be a violation of the national law implementing Directive 91/263/EEC on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity.

Appendix G
Warranty Statement

HARDWARE

Zaxus warrants that Product (excepting software products) supplied will be free from defect resulting from faulty manufacture or workmanship for 12 months from the date of delivery.

Product found to the Company's satisfaction to be defective will, at the sole discretion of the company, either be replaced free of charge or repaired free of charge provided that:

the Products (or samples thereof showing the alleged defects) are returned properly packed carriage paid to one of the Company's facilities at the customer's risk within 12 months from the date of delivery as defined in our normal terms and conditions of trading, and

the Products have not been misused mishandled overloaded amended modified or repaired in any way by the customer its servants or agents, or used for any purpose other than that for which they were designed, and

if the Products have been manufactured to the Customer's design the defects are not as a result of faulty design by the Customer.

Repaired or replaced Products will be returned free of charge to destinations within the country to which they were originally delivered or will be returned FCA (at Zaxus' nominated port) to other destinations.

This warranty is the only warranty given by the Company and specifies the entire liability of the Company including liability for negligence and in particular but without limitation all statutory or other express implied or collateral terms conditions or warranties are excluded.

NOTE

The limits on Zaxus' liabilities and a customer's legal rights as expressed in these warranties are applicable to the maximum extent allowed by the appropriate governing law in the customer's state or jurisdiction.