AEP Networks

General notes:

Set the key lock to the vertical position to allow the keypad to be used or to the horizontal position to disable the keypad and LCD.

SO refers to Security Officers. CO refers to Crypto Officers.

Cards or card refers to smart cards.

Smart cards

Security Officers:	sets of m of n Security Officer smart cards, each has a PIN
Crypto Officers:	sets of m of n Crypto Officer smart cards, each has a PIN
Operator:	sets of m of n Operator smart cards, each has a PIN
AAK:	sets of m of m smart cards each containing an AAK component
SMK:	sets of m of n smart cards each containing an SMK component
Application Key:	smart card(s) containing application keys
Configuration info:	smart card containing the API Settings/Alg Settings/FIPS mode

After a blank card has been used as a specific type it can only be re-used as the same type. For example an AAK card cannot be used as an SMK card but can be re-used for AAK backup.

The supported smart card is the GemAlto MPCOS-EMV R5 8000. Additionally the Keyper Plus supports cards generated by Keyper versions going back to the Keyper 9720 version 1.6.

PINs

Default PIN: 11223344

PIN that is asked for is the actual PIN and not the required PIN. Exception is on PIN change. If the PIN is entered incorrectly five times in a row the card is permanently locked.

USB

A single USB flash drive can back-up all Application Keys on a Keyper Plus.

Supported partition types:

FAT16

FAT32

Keys

AAK:	protects Operator, CO and SO cards
ISMK:	protects Application Keys inside the Keyper
SMK:	protects Application Keys backed-up on smart card or USB
Application Key:	keys generated and used when requested by the application

Network

The Keyper's default network settings are:

IPv4 Address:	192.168.0.2
IPv4 Subnet mask:	/24
IPv4 Default Gateway:	0.0.0.0
IPv6 Link-local Address:	fe80::<EUI-64 value derived from MAC address>
IPv6 Link-local Subnet mask:	/64
IPv6 Address:	2001::<EUI-64 value derived from MAC address>
IPv6 Subnet mask:	/64
IPv6 Default Gateway	::
Crypto API Port:	5000

Firmware downloads and audit extraction take place on port 3000.

Network Settings can be changed using the HSM Mgmt/Set Network menu options. After changing the settings the Keyper Plus should be power cycled.

States

The Keyper is always in one of the following states. 'Host' refers to the computer on which an application resides that uses the Keyper to generate keys, signatures etc.

Unsecure: not commissioned, no keys, default settings

Secure, Off-line: commissioned, ignores host requests, keys can be backed up/restored

Secure, On-line: commissioned, accepts host requests

Tampered (operational): commissioned, no keys, can be recovered by customer

Tampered (positive): no keys, can only be returned to Unsecure state by AEP

Download: commissioned, taking firmware update, ignores host requests

Unsecured to Secured

LCD: Displays 'Unsecured 9860' or ‘Important Read Manual’

READY LED: off

If the Keyper is to be managed by an existing sets of Operator and SO smart cards, select the following menu options in the following order:

- Import AAK
- Secure (changing the default settings) – press the restart button before proceeding

If the Keyper is the first to be configured or is to be managed by its own smart cards, select the following menu options in order:

- Issue SO Cards
- Secure (changing the default settings) – press the restart button before proceeding
- Role Mgmt
- Issue Cards (to issue Operator and Crypto Officer cards)
- Backup AAK

Secured Off-line to Secured On-line

LCD: Displays 'Secured 9860-2'

READY LED: off

Requires: - set of Security Officer smart cards and their PINs. (to automatically go on-line)
set of Operator smart cards and their PINs. (to manually go on-line)

To configure the Keyper Plus to automatically go on-line when the unit powers up:

- HSM Mgmt, Auto online
- Press ENT if it states 'Enable' on the second line of the LCD

To configure the Keyper Plus to not automatically go on-line when the unit powers up:

- HSM Mgmt, Auto online
- Press ENT if it states 'Disable' on the second line of the LCD

To set the Keyper Plus on-line:

- Set Online

Secured On-line to Secured Off-line

LCD: Displays 'Secured 9860-2'

READY LED: on

Requires: a set of Operator smart cards and their PINs or if 'Auto on-line' is disabled simply press the restart button or power cycle.

To set off-line select this menu option:

- Set Offline

FIPS to Non-FIPS

Requires: Set of SO smart cards and their PINs.

To set on-line select this menu option:

- Set FIPS Mode and then press ENT if it states 'Disable' on the second line of the LCD

Secured Off-line to Unsecured (Destroys Application keys)

LCD: Displays 'Secured 9860-2'

READY LED: off

Requires: Set of SO smart cards and their PINs.

To destroy all the key material i.e. application keys, SMK, AAK, select the following menu options:

- HSM Mgmt, Unsecure

Operational Tampered to Secured

LCD: Displays 'Clear Status?'

ALERT LED: on

Requires: Set of SO smart cards and their PINs.

Press ENT and insert the SO cards and enter their PINs.

Any to positively tampered (controlled)

Insert pin or paper clip in pin hole in rear of unit.

Tamper States

Causes:

Positive	outside temperature range, internal voltage out of tolerance or unit physically compromised
Operational	power supply outside tolerance or too rapid change in temperature
External (positive)	press pin in pin hole in rear of the unit

Recovery:

Positive	return to AEP for repair or recovery and re-commissioning
Operational	clear condition and restore SMK and Application keys
External (positive)	return to AEP for repair or recovery and re-commissioning

HSM Management

These are all options under the HSM Mgmt menu option.

Requires: Set of SO smart cards and their PINs to enter this menu system.

The Keyper should be Secured and off-line

LCD: Displays ' Secured 9860-2 '

READY LED: off

All menu option names are before the colon.

HSM Management menu:

Auto Online: allowing an online Keyper to stay online if power cycled

Change Clock: changing the real time clock

Set Network: change the network settings

View Cards: view smart card type and serial number

Unsecure: go back to unsecured state

Statistics: HSM and Crypto API performance

HSM Info: Details of the HSM settings and status

Non-authorised Operations

All are main menu operations:

HSM Info: details of the HSM settings

View Cards: view smart card type and serial number

Other

Requires the relevant smart card and the current PIN to carry this out:

Change PIN: change the PIN on an Operator, Security Officer, Crypto Officer or Configuration Information smart card

Role Management

These are all options under the Role Mgmt menu option.

Requires: Set of SO smart cards and their PINs to enter this menu system.

The Keyper should be Secured and off-line

LCD: Displays ' Secured 9860-2 '

READY LED: off

All menu option names are before the colon.

Role Management menu:

Issue Cards: issue sets of Crypto Officer and Operator cards

View Cards: view smart card details

Backup AAK: export a copy of the AAK to smart card

Clear RoleCard: remove the contents of a role card

Clear AAK Card: remove the contents of an AAK card

HSM Info: Details of the HSM settings

Operator

Requires: Set of Operator smart cards and their PINs to use these menu options:

Set Online: sets the Keyper on-line

Set Offline: sets the Keyper offline

Key Management

These are all options under the Key Mgmt menu option.

Requires: Set of CO smart cards and their PINs to enter this menu system.

The Keyper should be Secured and Off-line

LCD: Displays ' Secured 9860-2 '

READY LED: off

All menu option names are before the colon.

Key Management menu:

Key Summary: output the numbers of Application keys stored by type to the serial port

Key Details: for each stored Application key, output the key type, size, use and label to the serial port

App Keys: manage the Application Keys

SMK: manage the SMK

API Settings: switch on/off algorithm functions

Alg Settings: switch on/off non-Suite B algorithms

SMK sub-menu:

Generate SMK: generate a new SMK

Backup SMK: backup an SMK onto smart cards

Restore SMK: restore an SMK from smart cards

Clear Cards: clear the SMK from smart cards

View Cards: view the type and serial number of a smart card

App Keys sub-menu:

Backup: backup all or some Application keys to smart cards or USB

Restore: restore Application keys from smart cards or USB

Legacy Backup: backup Application keys to smart card so that Keyper Enterprise or Professional version 1.6 can read them

Legacy Restore: restore Application keys from smart card backed up by Keyper Enterprise or Professional version 1.6

Clear Media: clear the Application keys from smart card or USB

Media contents: send details of Applications cards stored on smart card or USB to the serial port

Erase App Keys: erase all Application keys from the Keyper

IMPORTANT:

Depending upon the provider used (PKCS#11, RSA Full Provider/SChannel Provider) the appropriate key mapping file MUST be backed up at the time the Application Keys are backed up. Failure to do so may result in the Application Keys being un-usable after being restored.

API Settings sub menu:

Enable or disable specific API operations:

Key Import: allow/disallow key imports

Key Export: allow/disallow key exports

Asym Key Gen: allow/disallow ECDSA/DSA/RSA key pair generation

Sym Key Gen: allow/disallow AES/triple DES key generation

Sym Key Der: allow/disallow triple DES key derivation

Signing: allow/disallow ECDSA/DSA/RSA private keys for signing

Verifying: allow/disallow ECDSA/DSA/RSA public keys for verifying signatures

MAC Gen: allow/disallow AES/triple DES keys for MACing

MAC Ver: allow/disallow AES/triple DES keys for verifying MACs

Enc/Dec: allow/disallow keys for encrypting/decrypting data

Asym Key Del: allow/disallow the deletion of ECDSA/DSA/RSA keys

Sym Key Del: allow/disallow the deletion of AES/triple DES keys

Alg Settings sub-menu:

Non Suite B: allow/disallow triple DES/DSA/RSA key use as a result of API calls