Ultra ELECTRONICS | AEP Networks

Ultra Safe

Keyper *PLUS* Model 9860 User Guide

Version: July 2013

Part Number	011429

Copyright

The information in this document is subject to change without notice and does not represent a commitment on the part of AEP Networks Ltd. AEP Networks Ltd does not accept any responsibility for any errors that may appear in this document.

The firmware and software described in this document is furnished under a license and may be used only in accordance with the terms of such license. The documentation is issued in confidence for the purposes only for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under an agreement or with the consent in writing of AEP Networks Ltd, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of AEP Networks Ltd.

All URLs given were active at the time of going to press. AEP Networks Ltd makes no guarantee of their continued validity and takes no responsibility for their content.

Proprietary Note

The information contained in this document is, to the best of our knowledge, entirely correct. However, AEP Networks Limited cannot accept liability for any inaccuracies or the consequences thereof, or for any liability arising from the use or application of any circuit, product, or example shown in this document. AEP Networks Limited reserves the right to change, modify, or improve this document or the product described herein, as seen fit by AEP Networks Limited without further notice.

Trademarks

Published July 2013

1st Issue

Ultra Electronics
AEP Networks
Knaves Beech Business Centre
Loudwater
High Wycombe
Buckinghamshire, HP10 9UT

Main Switchboard: +44 (0)1628 642 600

For further information about other Ultra AEP products, please visit our web site: www.ultra-aep.com

License and Credits

AEP Networks Ltd licenses the firmware inside AEP Keyper together with all supplied supporting host computer based software. By installing and/or using this product, you accept the terms and conditions of the current standard AEP Networks Ltd license agreement.

If you do not have a current copy of this agreement and would like to see it, please contact the AEP Networks Ltd contracts department. If you have a signed a license agreement with AEP Networks Ltd for this product, the terms and conditions of that signed license agreement take precedence over the standard terms and conditions.

Table of Contents

Declaration and statement of compliance

CE MARKING DECLARATION OF CONFORMITY

This digital apparatus complies with the requirements of the EC Directive 89/336/EEC, and amendments and the EMC low Voltage Directive 72/23/EEC and amendments.

The electro-magnetic susceptibility has been chosen at a level that gives correct operation in business and light industrial premises by its connection to the low voltage power supply system.

CANADIAN DEPARTMENT OF COMMUNICATIONS COMPLIANCE STATEMENT

This digital apparatus does not exceed the Class B limits for random noise emissions from digital apparatus as set out in the radio interference regulation of the Canadian department of communications.

DECLARATION DE CONFORMITE AU MARQUAGE CE

Le present appareil numérique est conformité avec les exigences des directives EC 89/336/EEC, amandées par les directives 93/95/EEC et 96/58/EEC, et est en conformite avec les exigences des directives EMC sur les basses tensions 73/72/EEC et l'amendement 93/68/EEC.

La sensibilité électro magnétique est à un niveau rendant les appareils propre à l'utilization en bureaux, industrie d'une alimentation électrique basse tension.

Declaration du Ministère des Communications du Canada

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Class B prescrites dans le règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Safety information

SAFETY

This equipment has been designed, manufactured and tested to meet Safety Standards for data processing equipment; however, as with any electrical apparatus, care must be taken when using it.

This equipment MUST only be used with the PowerSolve PSGE65-12-01 mains-DC converter (PSU) module supplied.

WARNING: Attempting to open the module can create the danger of electric shock.

The mains lead provided must be plugged into an earthed mains outlet; the mains outlet should be close to the equipment and permanently accessible for emergency disconnection.

Only the mains cord supplied or an equivalent cord that complies with local regulations should be used.

This unit contains a Lithium Battery with potential fire, burn and explosion hazards.
Do NOT subject the unit to extreme heat (above 100°C) or cold (below -50°C).
Do NOT dispose of the unit by landfill or incineration; return to AEP Networks Ltd for recycling.

Do NOT install the equipment in a manner that will obstruct the free flow of air over its upper surfaces. If it is rack mounted, the recommended vertical spacing interval is 2U (88mm).

Before moving or installing the equipment, positively disconnect the power lead at the mains outlet.

CONSIGNE DE SECURITE

Cet matériel a été conçu, fabriqué et testé pour répondre aux critères des standard internationaux de sécurité pour les matériels électroniques; cependant, comme tout appareil électrique, il doit être utilisé avec précaution.

Cet équipement doit être utilisé exclusivement avec le cordon d'alimentation et le transformateur électrique fournis avec le produit.

AVERTISSEMENT, essayer d'ouvrir le transformateur peut entraîner un choc électrique.

Le cordon d'alimentation fourni doit être branché dans une prise d'alimentation électrique avec terre; la prise d'alimentation électrique doit être proche du matériel et accessible en permanence pour pouvoir être rapidement débranchée en cas d'urgence.

L'unité contient une pile au lithium entraînant des risques potentiels d'incendie et explosion.
L'unité ne doit pas être soumise à des températures extrêmes (supérieures à 100°C ou inférieures à 50°C).

L'unité ne doit pas être mise en décharge ou incinérée mais retournée à AEP Networks Ltd pour être recyclée.

L'unité ne doit pas être installée de manière à bloquer la circulation d'air autour des faces supérieures du boitier. Dans le cas où les unités sont empilées, l'espace vertical minimal recommandé est de 88 millimètres.

Avant tout déplacement or installation du matériel, le cordon d'alimentation doit être débranché de la prise d'alimentation électrique.

Explanation of Symbols

The following table lists conventions that are used throughout this guide.

Icon	Notice Type	Description
CE	**CE Conformity**	This symbol indicates that the product described in this manual is in compliance with CE standards.
ℹ	**Information note**	Information that describes important features or instructions.
⚠	**Important**	Information that alerts you to important information.
⚠	**Warning**	This symbol and title emphasize points which, if not fully understood and taken into consideration by the reader, may endanger your health and/or result in damage to your material.
⚡	**Caution, Electric Shock**	This symbol and title warn of hazards due to electrical shocks (> 60V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material. See also High Voltage Safety Instructions section.

1 Introduction

The AEP Networks Keyper ^{PLUS} Model 9860 is a general purpose HSM that is optimised for applications requiring the use of Suite B algorithms.

The Keyper provides strength, performance and world beating levels of security for the generation, storage and use of cryptographic keys for use in mission critical applications such as Certification Authority (CA), Validation Authority (VA) and smart card issuing systems.

The Keyper is a stand-alone unit with a separate power supply. It has an integrated keypad that can be folded into the chassis, back lit display, additional indicators, a physical key switch, USB memory socket and a smart card reader.

Cryptographic facilities implement industry standard algorithms covering signatures, encryption, MACing, secure key storage and key management.

Only key material can be stored in Keyper; non-key material such as certificates or temporary data cannot.

The host machine contains application software requiring access to cryptographic services via a driver providing access to RSA's PKCS#11 v2.11/v2.20 API.

This user guide covers the following products/drivers:

	Model	**Release/version**
Keyper ^{PLUS}	9860	2.2

Return to factory

In the unlikely event that Keyper requires returning to AEP Networks Ltd for maintenance, it should be returned to 'Unsecured State'' before shipping. A menu option, authorised by security officers, is provided for this purpose. When this option is selected all application and smart card protection keys are destroyed and the network configuration cleared. If the security officer smart cards have been destroyed or damaged, the unit can be safely tampered by entering a pin into the pin hole on the reverse of Keyper.

Protection of key material

Possession of the cryptographic keys would make it easier for an attacker to decrypt the data transmitted by Keyper. For this reason, cryptographic keys must be carefully protected. Any material, paper records, non-volatile magnetic or magnetic media, containing the keys must be stored under lock and key. The cryptographic key material should be treated as information, bearing a sensitivity marking at least as high as the most sensitive information protected by Keyper.

Protection against theft

On power up, a Security Officer must authorise the Keyper to accept requests from the host for cryptographic services. A menu option is provided for this purpose.

Protection against unauthorised use

When powered down or reset a Keyper restarts with cryptographic services shut-down.

Handling of incidents

All reported failures of the communications link protected by Keyper should be followed-up immediately.

It is good practice to log all incidents causing communications link failures.

2 Keyper Concepts

The Keyper's first and foremost design objectives are to be secure and reliable. It is very sensitive to misuse because misuse can be taken to be an attack.

The Keyper is a network attached unit. Applications communicate with it via an AEP produced 'Provider'. This hides the Keyper and the network from the Application. Key management operations take place via its built in keypad/LCD and smart card reader.

A 'Provider' can be one of the following:

- PKCS11 Provider: implements the industry standard PKCS#11 API
- RSA Full Provider: implements the variant of Microsoft's CAPI that is used by Microsoft Certificate Services
- SChannel Provider: implements the variant of Microsoft's CAPI that is used by Microsoft IIS

The following guidelines may help in selecting a Provider. The reader should research for themselves the API that best fits their requirements.

API	Strengths	Weaknesses
PKCS#11	Industry Standard, platform independent Supported by nearly all enterprise level third party applications such as Certificate Authorities, Validation Authorities, Registration Authorities etc. Offers the ability to secure keys using key	Complex API to write software for

API	Strengths	Weaknesses
	policies (export/no export etc.) Best API to use for devices containing a key store Most algorithm support	
Microsoft CAPI	Used by Microsoft products X.509 certificate issuing is supported	Only available for Microsoft Windows 2003 and later No SHA-2 support No ECDSA, ECDH support No AES support Not much third party support Key policies are limited It is now effectively obsolete

AEP's providers are in the form of shared libraries that are loaded by a third party Application. At that point the shared library sets up connections to the Keyper (up to 256 connections can be made into a Keyper). The Application can then make calls into the shared library which passes those calls down into the Keyper usually via port 5000 (this is configurable).

The Keyper does not support DHCP so it must be given a fixed IP address. It does not support DNS, SNMP or SMB; it is not standard computer hardware. The Provider must be configured with the Keyper’s IP address and port.

The Keyper will not accept any calls if it is offline.

When a Keyper is shipped it is in Unsecured State. It is not secured in the sense that there are no valid Security Officers at this point.

Security Officer cards are required to secure the Keyper. Security Officer cards can be issued while the Keyper is in Unsecure state or pre-existing Security Officer cards can be used if the AAK associated with those cards is first imported into the Keyper.

The principle of the Keyper is that all security related functions require at least two Operator smart cards to set the unit on/off line, at least two Security Officer smart cards to carry out HSM / role management and at least two Crypto Officers to carry out key management.

Keys generated as a result of a key generation request from an Application or keys imported from smart card are called Application keys. Application keys stored internally are protected by the ISMK key. When exported they are protected by the storage master key (SMK). The SMK can be exported so that the SMK may be imported to different Keypers allowing Application keys to be transferred between Keypers..

If the Keyper suffers a positive or an operational tamper the ISMK, SMK and the work area containing temporary plain text keys are positively destroyed. Application keys are destroyed.

Positive tampers additionally destroy the IMK making the Keyper completely unusable.

3 Key Hierarchy

There are three categories of keys within the Keyper key hierarchy:

- Authorisation key (AAK)
- Storage Master key (internal – ISMK and transport - SMK)
- Application keys (App. Keys)

The Authorisation Key (AAK) is the key that protects the Operator, Security Officer and Crypto Officer smart cards. These smart cards are only tied to the AAK (and vice-versa) and to no other key.

The role of the Operator, Security Officer and Crypto Officer smart cards are to protect the Keyper from unauthorised use.

The SMKs and Application Keys are related to each other but are not tied to any other keys. The SMKs exist to protect Application Keys internally (ISMK), and when backed up on smart card / USB (SMK), or exported via the communications interface (SMK).

Application Keys are the keys generated by Keyper on demand from the application via the PKCS#11 Provider or RSA Full Provider/SChannel Provider implementation. For example, a CA Root Signing Key is an Application Key.

Authorisation key (AAK) and Operator/Security Officer/Crypto Officer smart cards

Operator, Security Officer and Crypto Officer smart cards are collectively referred to as role cards.

The Authorisation Key (AAK) protects Keyper from unauthorised access by providing the means to authenticate role cards. There is only one AAK. It is either generated by a Keyper and or imported from another Keyper. The AAK is stored as a set of smart cards which have to be presented to re-create the key. Each smart card contains one component.

Each role card is associated with a single AAK. Role cards are issued in sets. On issue, each role card contains information on which set it belongs to and the type of role card. This information is protected by the AAK.

To use a set of role cards with a Keyper, the Keyper must contain the AAK associated with the role card set.

AAK Smart Cards

It should be noted that the way the AAK is managed between Keypers is an important decision in the deployment process.

The AAK is imported/backed up in “M of N” component form. All the exported components are required to re-create the key.

M (components required to re-build AAK)	N (components exported)
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9

An AAK backed up from one Keyper unit can be imported into another. All of the component smart cards are required to rebuild the key.

Back up

Once the unit is in Secured State' the AAK can be backed up at any time.

Restore

The AAK can only be restored while the Keyper is in 'Unsecured State'**.** Refer to Keyper in the section 'Keyper in Unsecured State' for more information.

Operator, Security Officer and Crypto Officer Smart Cards

Role cards are issued in sets of “M of N” cards where “M” cards are required to authenticate an operation out of “N” cards issued in the set. At least two cards must be issued (2 of 2) but as many as 9 can be issued (9 of 9). Examples of sets of cards are 2 of 4, 3 of 8, 2 of 8 and 5 of 6.

M (smart cards required to authorise card functions)	N (smart cards in a set)
2	2/3/4/5/6/7/8/9
3	3/4/5/6/7/8/9
4	4/5/6/7/8/9
5	5/6/7/8/9
6	6/7/8/9
7	7/8/9

8	8/9
9	9

All smart cards have a PIN at all times. The PIN that is asked for is the actual PIN unless the 'Change PIN' menu option is selected in which case the old and the new PIN must be asked for.

Smart cards issued in separate sets cannot work with smart cards from a different set.

Storage Master Key (SMK)

The purpose of the external Storage Master Key (SMK) is to wrap the Application Keys for exporting out of the Keyper. See “Application Keys” for more information.

To transfer Application keys between Keypers it is necessary for both Keypers to have the same SMK. Therefore the way the SMK is managed between Keypers is a key decision in the deployment process.

An option is provided to disallow any key export at all. If this option is selected (no export) the SMK cannot be imported, backed up or generated.

The SMK is backed up using the M of N methodology. This enables the SMK to be backed up in component form, one component per card. The SMK is broken into N components for export. M of those components are required to re-build the SMK. A minimum of 2 (M) of 4 (N) cards to a maximum of 9 (M) of 9 (N) cards are required to rebuild the SMK.

The M of N options are as follows:

M (components required to re-build SMK)	N (components exported)
2	4/5/6/7/8/9
3	4/5/6/7/8/9

4	4/5/6/7/8/9
5	5/6/7/8/9
6	6/7/8/9
7	7/8/9
8	8/9
9	9

This method allows flexibility. For example, if three copies of an SMK are required select 3 of 8 and keep four sets of two components in separate backup furniture. This will ensure that no single piece of furniture holds enough components to recreate an SMK while at the same time allowing an offsite backup and one spare smart card in every four should a smart card fail.

Generate new Storage Master Key

This feature is not available if Key Export is disabled.

If the Keyper changes from Unsecured State to Secured State a new SMK will be automatically generated.

To generate a new SMK the following process should be followed, using supplied menu options for each:

1. Shut-down cryptographic services
2. Generate SMK
3. Start-up cryptographic services

Backup

This feature is not available if Key Export is disabled.

To back up an SMK the following process should be followed, using supplied menu options for each:

1. Shut-down cryptographic services
2. Back up onto smart cards
3. Start-up cryptographic services

⚠

It is essential that the SMK has been successfully backed-up otherwise it will not be possible to import Application Keys to other Keypers or to the same Keyper if it has been unsecured or tampered.

After the SMK has been written to a set of smart cards the user is required to re-insert each card so that each M of N combination can be verified.

Restore

This feature is not available if Key Export is disabled.

An SMK can be restored at any time and as many times as required.

The Keyper supports one AES SMK and one TDES SMK. Both SMKs can be restored regardless of which SMK type was selected when the Keyper was Secured. This allows application keys which have been backed up with either type of SMK to be restored.

To restore an SMK the following process should be followed, using supplied menu options for each:

1. Shut-down cryptographic services
2. Restore SMK
3. Start-up cryptographic services

⚠ ***IMPORTANT:*** *Great care should be taken to back up the SMK after generating it but before backing up the Application Keys.*

To transfer Application keys between Keypers it is necessary for both Keypers to have the same SMK.

Application keys

Application keys are keys generated by a request for cryptographic services, that is, a key generation request by a host application.

⚠ ***IMPORTANT:*** *Note that it is important which mode the Keyper is in when keys are generated. If the Keyper is in FIPS mode only keys that are generated to FIPS standards can be generated. Non-FIPS approved generation (i.e. key derivation) is prohibited while the unit is in FIPS mode.*

FIPS keys can only be used for FIPS approved purposes. Non-FIPS keys cannot wrap or unwrap keys generated in FIPS mode.

Protected keys consist of key material, key policy and a key identifier; all of which are wrapped by the SMK while exported.

The Application Key store can be backed up onto smart cards or onto a USB memory stick and restored in the same way. Individual Application Keys, and subsets of Application Keys, can be identified, and therefore backed up. However, individual keys are identified by their label. These labels are the first seven characters of the PKCS#11 key label or the Microsoft CAPI container name. For keys to be individually identified sensible, unique, human readable names must be given to keys when they are generated. However, be aware that few third party applications set human readable names.

Application keys can be transferred between different versions of Keyper. Please refer to Application Key Back-up and Restore for details of which keys can be moved between which versions.

The options to backup and restore Application Keys are not available if Key Export is disabled.

Cryptographic services must be halted via the menu option before any back up or restoration of Application Keys is undertaken. The message 'ACCESS DENIED' will be displayed if this is not done.

Application keys should be backed up and restored in step with the PKCS11Provider data file. The PKCS11Provider data file holds a mapping of the API key id for each Application Key and the unique key id for that Keyper. If this data file is out of step with the Keyper key store the application will not be able to access the keys. The PKCS#11 Provider, RSA Full Provider and SChannel Provider all use common data files allowing them to share keys.

For example it is possible to generate a key pair using the PKCS#11 Provider and then to use that generated private key using the RSA Full Provider.

Backup

This feature is not available if Key Export is disabled.

Backing up is a two-stage process. On selecting the backup option from Keyper, the backup media is prompted for i.e. smart card or USB memory stick. It is recommended to only use smart cards if small numbers of keys are to be backed up (i.e. less than 5 2048 bit RSA keys or less than 10 256 bit ECDSA keys). Otherwise use a USB memory stick.

If smart cards are selected as the backup media:

1. Select the keys to be backed up (all or a selection of the keys in the key store)
2. Each card required is prompted for, formatted and copies of the selected Application Keys written to the smart cards until all the selected keys have been backed up

If a USB memory stick is the preferred back up media:

1. Select the keys to be backed up (all or a selection of the keys in the key store)
2. The USB memory stick required is prompted for, formatted and copies of the selected Application Keys written to the USB memory stick until all the selected keys have been backed up – note that only one USB memory stick will be asked for.

Progress of the Application Key back up can be followed by monitoring the audit events that are output from the serial port.

It is crucial that the SMK that protects the Application Keys is backed up (see Storage Master Key for more information).

In brief, to back up Application Keys the following process should be followed using supplied menu options for each:

1. Shut-down cryptographic services
2. Back up the SMK if it has not already been done - see ‘Back up SMK’ for more information
3. Back up the Application Keys
4. Back up the PKCS11 Provider data file from the host
5. Start-up cryptographic services

***IMPORTANT:* Keyper performs a read after write test when writing to backup media to confirm that they have successfully been written to. However, after backing up Application Keys it is good practice to check that they can be restored to confirm the integrity of the back-up media.**

Restore

This feature is not available if Key Export is disabled.

The SMK must be the SMK used to protect the Application Key backup.

Each Application Key backup media contains a “whole” number of keys. Application Keys are not split across multiple smart cards or USB memory sticks. Keys are imported one smart card at a time so if the second smart card fails the others can still be recovered. In the case of USB memory sticks, only one is prompted for.

If the error code '120d' is displayed the SMK in Keyper is different from the SMK which wrapped the Application Keys being restored.

In a multiple host scenario, the PKCS11Provider data file is not synchronized between hosts. Such synchronization is a manual process.

In brief, to restore Application Keys the following process should be followed, using supplied menu options for each:

1. Shut-down cryptographic services
2. Restore the SMK first from smart cards if it has not already been done (see the section on Restoring the Storage Master Key for more information)

3. Restore the Application Keys from the backup media into the Keyper
4. Recover the PKCS11Provider data file to the host
5. Start-up cryptographic services.

4 Security Mechanisms

A number of security mechanisms are employed by Keyper to protect its integrity:

- Security Roles
- Controlled initialisation
- Authorised acceptance/rejection of requests for crypto services
- Authorised acceptance/rejection of requests for on-line import/export of keys
- Authorised acceptance/rejection of requests for crypto operations
- Authorised acceptance/rejection of requests for crypto algorithms
- Authentication of requesters of crypto services
- Authorised and audited key management including secure key import/export
- Authentication of software updates
- Two stage tamper detection
- Hardware failure detection

Security roles

The Keyper is protected by the following levels of Authorisation:

- Between two (and nine) required of between two (and nine) issued Operator smart cards

- Between two (and nine) required of between two (and nine) issued Security Officer smart cards
- Between two (and nine) required of between two (and nine) issued Crypto Officer smart cards

This requires individuals to be assigned to perform the following basic roles:

- Operator
- Security Officer
- Crypto Officer
- Key component holder
- Application Key holder
- Configuration Data holder

It should be noted that it is possible to carry out a few non-security related operations without being authorised.

These operations are:

- View smart card types
- View the network settings
- Output the configuration/state via the serial port
- View the FIPS mode
- View the firmware version number

Consideration is needed to determine who will fulfill these roles and to develop procedures to provide the required level of security.

Operator (OP)

Purpose: to make the Keyper available for remote cryptographic operation.

Operators(s) are authenticated by the insertion of their smart card followed by the PIN associated with that smart card. A set of Operator smart cards (and their PINs) are required to:

- Set the Keyper on line
- Set the Keyper off line

⚠ ***IMPORTANT:*** *Note that smart cards allow an incorrect PIN to be entered four times in succession. If the PIN is entered incorrectly a fifth time the smart card cannot be used or recovered by the user or by AEP Networks.*

Security Officer (SO)

Purpose: to change the configuration of the Keyper and to issue Role cards.

Security Officers are authenticated by the insertion of their smart card followed by the PIN associated with that smart card. A set of Security Officer smart cards (and their PINs) are required to:

- Back up AAK keys onto smart cards
- Restore AAK keys from smart cards
- Clear AAK and Role smart cards
- Issue Operator smart cards
- Issue Crypto Officer smart cards
- View an inserted smart card’s details
- Set the time and date of the Real Time Clock
- Unsecure a Keyper to the state it was in when it was delivered, e.g. delete AAK, all Application Keys, SMKs and network configuration

- Clear an operational tamper indication
- Set the FIPS mode
- Configure the network settings

⚠ ***IMPORTANT:*** *Note that smart cards allow an incorrect PIN to be entered four times in succession. If the PIN is entered incorrectly a fifth time the smart card cannot be used or recovered by the user or by AEP Networks*

Crypto Officer (CO)

Purpose: to manage the backup, restoration and deletion of keys on the Keyper.

Crypto Officers are authenticated by the insertion of their smart card followed by the PIN associated with that smart card. A set of Crypto Officer smart cards (and their PINs) are required to:

- Back up SMK keys onto smart cards
- Restore SMK keys from smart cards
- Back up Application Keys to smart cards or USB memory sticks
- Restore Application Keys from smart cards or USB memory sticks
- Clear SMK and Application smart cards or USB memory sticks
- View an inserted Application key USB memory stick or smart card’s details including key identification details
- Delete Application Keys from inside Keyper
- Enable/disable command types issued by the PKCS#11 Provider/CAPI by algorithm and function (e.g. key import, key generation, signing)
- Output a list of key labels held in the Keyper's key store via the serial port
- Output a summary of the number of keys held in the Keyper's key store, by algorithm, key types and key sizes via the serial port

⚠ ***IMPORTANT:*** *Note that smart cards allow an incorrect PIN to be entered four times in succession. If the PIN is entered incorrectly a fifth time the smart card cannot be used or recovered by the user or by AEP Networks*

Key Component Holder

A key component holder holds one or more smart cards in a set. Security Officers (AAK) or Crypto Officers (SMK) are required to authorise Key Component owners to restore the AAK or SMK.

Application Key Holder

An Application Key holder holds the smart card(s) or a USB memory stick containing backed up keys. Each smart card/USB memory stick is inserted into a Keyper to backup or to restore keys. Crypto Officers must first authorise this operation.

Controlled initialisation

On delivery Keyper is not secured because at that point no Security Officer smart cards have been issued for that unit. AEP does not issue Security Officer smart cards. They are issued and owned by the owners of the Keyper.

Keyper is in a "controlled" Unsecured State on delivery. In this state an Authorisation Key (AAK) can be imported. If an AAK is not imported, one is automatically generated when the Security Officer smart cards are issued. An automatically generated AAK must be persisted by Securing the Keyper.

Once imported or automatically generated, the AAK can be used to issue multiple sets of Security Officer cards. Security Officer smart cards can only be issued when the unit is in Unsecured State.

When the Keyper is powered up in Undescured State the message ‘IMPORTANT READ MANUAL’ is displayed. At this point anyone who powers up the unit can control it.

⚠ ***IMPORTANT:*** *If Keyper is not in Unsecured State on delivery, assume that it has been compromised* *and return it to AEP Networks.*

It is possible for a Keyper to have generated an AAK and issued Security Officer smart cards even if delivered in an Unsecured State. However, on powering down the Keyper the AAK is destroyed rendering any issued smart cards useless.

In Unsecured State Keyper cannot accept any requests for crypto services. No SMK or Application Keys can be imported until Keyper is Secured.

A set of Security Officer smart cards must be used to switch to Secured State. Once this has been achieved 'Secured 9860-2' is displayed.

To conclude, a Keyper delivered in 'Secured' state is compromised. A Keyper delivered in Unsecured State is not. Keyper signals its condition on power up displaying 'IMPORTANT READ MANUAL' if in Unsecured State and 'Secured 9860-2' if in Secured State.

A set of Security Officers can return Keyper to Unsecured State by using the menu option 'Unsecure'. If selected, the Keyper destroys the AAK, SMK, all Application Keys, and the network configuration. All configuration settings are returned to their default values. When Keyper is powered up again, it will be in Unsecured State.

Authorised acceptance/rejection of requests for crypto services

A Keyper powers up off-line by default unless it has been positively configured to go on-line. When off-line the Keyper allows local management operations but refuses all requests for crypto services. This is to prevent keys stored on a stolen, Secured Keyper to be used without Operator authorisation. Even if an Operator smart card is accidentally left in the reader the thief still requires the card's PIN and at least one other Operator card and its PIN.

A Keyper can be set off-line at any time using a set of Operator smart cards. Setting a Keyper off-line is a prerequisite for a number of local management services such as restoring Application Keys or an SMK.

The Keyper can be configured to power up on-line automatically. Configuring this state requires authorisation by a set of Security Officer smart cards. This state leaves the Keyper in a more vulnerable condition so should only be used if the Keyper is in a secure location.

Authorised acceptance/rejection of requests for on-line import/export of keys

While a Keyper is on-line, the host computer can send cryptographic requests such as sign/wrap to Keyper. If the key that is the subject of a 'wrap' request allows export in its key policy, the wrap request (encryption of a key) will allow that key to be extracted via the network to the host computer.

This can be prevented by either generating the key with a 'no export' policy, which can be restrictive or by Crypto Officers entering the 'Key Mgmt' menu option to use the 'API Settings' sub-menu option 'Key Export' to disable all key exports via the API.

Enabling or disabling remains in force until changed.

If 'Key Export' is disabled while Keyper is in the 'Unsecured State', this overrides the other key export options (i.e. the key policy and the key export menu options) and it cannot be subsequently changed to ‘enabled’ without losing all of the keys in the Keyper.

The default settings are:

- Key Export is enabled
- Key Export via API is enabled

Authorised acceptance/rejection of requests for crypto operations

All API crypto operations can directly or indirectly enabled or disabled by a set of Crypto Officer cards. The following operations can be enabled / disabled:

- Key Export via API
- Key Import via API
- Asymmetric Key Generation

- Symmetric Key Generation
- Symmetric Key Derivation (in Non-FIPS mode)
- Signing
- Signature Verification
- MAC Generation
- MAC Verification
- Encryption/Decryption
- Asymmetric Key Deletion
- Symmetric Key Deletion

All operations are enabled by default.

Authorised acceptance/rejection of requests for crypto algorithms

Two types of algorithms are supported:

- Suite B (AES, ECDSA, ECDH, SHA-2)
- Non-Suite B (Triple DES, DSA, RSA)

Suite B algorithms are always enabled. The non-suite B algorithms are enabled by default and can be disabled by a Crypto Officer.

Authorised and audited key management

All key management functions require authorisation by a Crypto Officer and are audited.

Authentication of firmware updates

The Keyper must be on-line before its firmware can be updated.

Keyper verifies the signature on a download to authenticate that the firmware originates from AEP Networks.

The Keyper cannot be upgraded with an earlier version of firmware.

If any of these conditions are breached the download is rejected and the existing firmware is retained. All breaches are recorded in the audit log.

The Keyper Management Centre, which performs the download, requires the IP address and the serial number of the target Keyper to ensure the correct unit is being updated.

⚠ ***IMPORTANT:*** The power must not be removed, nor the process interrupted, while the Keyper is being updated.

Two stage tamper detection

The Keyper contains a tamper resistant internal module, which has features to prevent access to the cryptographic keys. Tamper detection is activated whether or not the Keyper is powered up.

Tamper conditions

There are two kinds of tamper:

- Positive tamper
- Operational tamper

Operational tampers are logged in the audit-log, See the appendix on error codes for a full list of tamper codes.

Both kinds of tamper result in the destruction of the SMKs and all keys held temporarily in plain text. The protected key store, including the Application Keys, will be rendered useless by the destruction of the ISMK and SMK.

Positive tamper

These events will cause a positive tamper:

- A physical breach
- Total power failure (mains power and battery)
- Temperature goes out of storage temperature range
- A pin is pushed into the pin hole at the rear of the unit

Keyper detects physical access by drilling, grinding, electrical tamper via the input, output and power signals and excessively low or high temperatures outside its operating range.

A cryptographic protection mechanism protects Keyper from unauthorised software download until it can be returned to AEP Networks. A positive tamper results in no unencrypted (i.e. recoverable) material existing within Keyper. Neither the AAK nor any material created after the Keyper was Secured will exist in the unit in any form after power on.

A Keyper that has been subject to a positive tamper is inoperable and will need to be returned to AEP Networks for repair/re-commissioning as appropriate.

Operational tamper

These events will cause an operational tamper:

- Power goes out of operating range
- Temperature goes out of operating range

The Keyper can be recovered by clearing the tamper condition through the supplied menu option, re-importing the SMK and restoring the Application Keys from smart cards or a USB memory stick (see ‘Resetting the tamper indicator’ for more information on recovery).

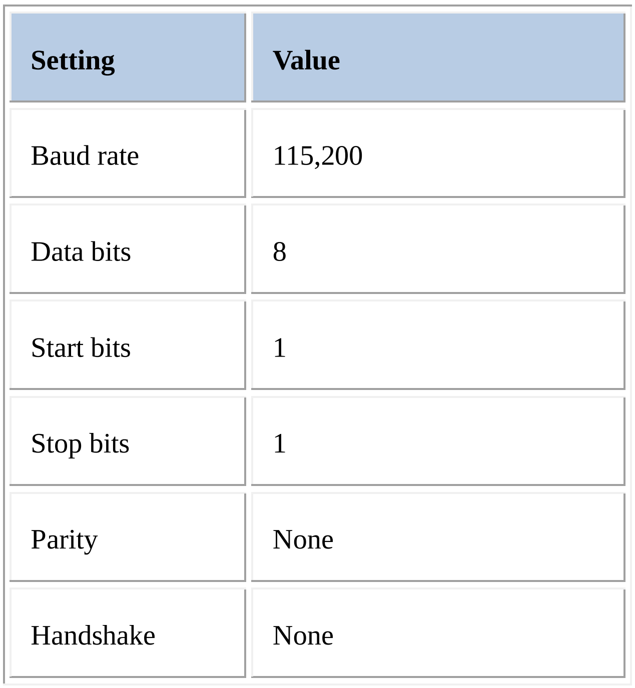
Hardware failure detection

When the hardware boots it performs diagnostic checks on the Level 1 Cache (L1), DRAM and then Level 2 Cache (2). If a failure is detected the boot software attempts to initialise the serial port to output an error message and then will stop booting.

In the unlikely event that an error should occur the Keyper should be returned to AEP Networks for repair. Contact AEP Networks support: techupport@ultra-aep.com

To view these error messages connect a serial terminal (for example, HyperTerminal running on a PC) to the serial port on the Keyper.

The serial port should be set up as follows:



Setting	Value
Baud rate	115,200
Data bits	8
Start bits	1
Stop bits	1
Parity	None
Handshake	None

For information, these are the relevant connector pin-outs for a standard PC 9 way D-type to PC 9 way D-type serial cable:

Keyper 9 way D-type	**PC 9 way D-type**
2	3
3	2
5	5

5 Getting Started

The Keyper should now be installed as detailed in the companion Keyper Installation Manual part number 010577. Once installed, Keyper should be continuously powered on.

The Keyper's features are:

- Back-lit LCD used for display of status information
- 20 key hexadecimal keypad for entry of PINs and basic configuration information
- Smart card reader for entry of key material from a smart card
- Key switch
- LED Indicators for line activity, power, ready, alert for key status
- Restart button
- USB Memory Slot

Features of Keyper

The following sections describe the various features of Keyper.

Liquid crystal display (LCD)

The liquid crystal display (LCD) is a 2 x 16 matrix display. Together with the keypad, this provides the user interface to Keyper. The LCD displays an extended ASCII character set and features a cursor. The LCD is lit by a 'back light' when Keyper is connected to the PSU.

The keypad and menu operation

The keypad has keys for the hexadecimal numbers 0-9, A-F. These are used to for menus operations.

The user interface menus can be navigated using the <, >, CLR and ENT keys on the control panel:

<**:** Scrolls the menu back if there are previous menu items. It moves the cursor left on data entry.

>**:** Scrolls the menu forward if there are more menu items. It moves the cursor right on data entry.

CLR: Exits the current operation and returns to the previous menu.

ENT: Confirms an operation and moves onto the next stage.

Menu items are selected by entering their corresponding number or letter on the keypad or by pressing ENT when displayed.

Note that menus are subject to a time-out. While in the Secured State, if a key is not pressed within 10 minutes of the previous key, the main Secured 9860 menu is re-displayed and any authorised access by Security Officer or Crypto Officer smart cards is cancelled.

Smart card reader

A smart card reader is located behind the front panel fold down flap.

Key switch

The key switch is located under the front panel fold down flap. The key switch enables the Keypad and the display,

Power LED

The green POWER LED is located at the bottom left of the display and is lit to show that Keyper is receiving a DC supply from the PSU.

Software driven LEDs

The front panel of Keyper contains a further eight LEDs that are lit in response to software commands, as follows:

READY: This is a green LED located in the middle of the front panel under the display. If READY is lit Keyper is available for cryptographic requests, Otherwise Keyper has stopped its network service.

ALERT: This is a red LED located to the right under the display. If the ALERT LED is lit, a tamper is occurring or has occurred.

(LAN) LINK: This is a green LED, lit to show that Keyper is connected to the network and that a link has been established. If the LED is not lit, a fault exists. Check that the correct cable connects Keyper and the host, namely:

A cross over cable to connect Keyper to an MDI network port on a host computer LAN card

A standard cable should be used to connect Keyper to an MDIX port on a hub or a switch

If the correct cable is being used, check that the cable is properly connected. If necessary, disconnect the cable, check for contamination on the plug/socket that may degrade performance and reconnect the cable.

(LAN) TX: This is a yellow LED located under the LINK LED, lit to show that Keyper is transmitting data onto the network.

(LAN) RX: This is a yellow LED located under the TX LED, lit to show that Keyper is receiving data from the network.

Three further LEDs (WAN) are located to the right of the LAN LINK, TX and RX LEDs. These are unused.

Restart button

The orange Restart button is located under the fold down flap. Keys are not erased.

Network connectors

An RJ45 connector, marked LAN, is located on the rear panel to enable connection to the network.

A second RJ45 connector, marked MGMT, is unused in this version.

Serial port

The 9-pin, D-type, serial port, marked AUX is for local audit event detection.

USB Slot

This is a USB 2.0 slot of the front of the unit. It is only used for backing up/restoring Application keys to/from a USB memory stick.

Power DC connector

The POWER DC input connector enables DC power to be applied to Keyper, via the in-line PSU.

Power supply unit

The PSU is an in-line mains power to DC converter, manufactured by PowerSolve, model number PSGE65-12-01, with the following dimensions:

Height - 32 mm

Width - 53 mm

Length - 117mm

The PSU is connected to the mains supply via the mains cord supplied. Only the mains cord supplied or an equivalent cord that complies with local regulations should be used. The DC output from the PSU is to the Keyper, at the POWER DC connector, via a lead, terminated in a standard 2-pin coaxial power connector.

The PSU provides a DC supply of +12V (max 5.42A). It requires an AC supply of between 100 VAC and 240 VAC (max 1.7A), in the frequency range 50 Hz to 60 Hz. The maximum power consumption of the equipment is 11 W.

Tamper detection

Keyper contains a tamper resistant internal module, which has features to prevent access to the cryptographic keys. Tamper detection is activated whether or not power is applied to Keyper. See the section on tampers and Security Mechanisms for details.

Internal battery

An internal battery is provided to protect the keys when Keyper is powered down. This battery has a manufacturer’s shelf life of at least 10 years. AEP Networks recommend that it is changed every 5 years.

The battery cannot be changed in the field. Keyper must be returned to AEP Networks.

6 Keyper in Unsecured State

A Keyper is in Unsecured State when it is shipped from AEP Networks. This is to ensure that at that point the Keyper cannot be controlled by any currently issued Operator/Security Officer/Crypto Officer smart cards, contains only default settings and that it contains no application keys.

When a Keyper is powered up in Unsecured State it cannot be used for any cryptographic operations. The ISMK and SMK do not exist and cannot be restored while in Unsecured State.

When powered up in Unsecured State the following will be shown on the LCD display:

```
Important

Read Manual
```

Followed by:

```
Unsecured 9860     >

1.Issue SO Cards
```

The 'Unsecured' on the top line indicates that Keyper is in the Unsecured State. The number shows which variant of Keyper is being used. 9860 refers to the Keyper Model 9860.

Pressing > will scroll to the next menu item.

Pressing < will scroll to the previous menu item, this menu has the following options:

```
Unsecured 9860    >
1.Issue SO Cards
2.Restore AAK
3.Secure
4.Key Export
5.HSM Info
6. Identify Cards
```

To select a menu item either:

- press its associated number
- use the scroll keys to select the menu item and press the ENT key

Pressing the CLR key will return you to the previous menu.

Unsecured State: Issuing Security Officer smart cards

Security Officer smart cards (SO smart cards) are issued in set of between 2 of 2 and 9 of 9.

Without a valid set of these cards a Keyper cannot be secured (i.e. set to Secured State). It should be noted that this menu option is the only option that allows Security Officer smart cards to be issued. It is recommended that multiple sets of Security Officer smart cards are issued, and for live systems that they are issued in a 3 of 8 set.

When Keyper is powered up for the first time, it will be in Unsecured State. In this state no Authorisation is required to issue sets of Security Officer smart cards. After these smart cards are issued select Secure.

1. Select Issue Cards from the Unsecured menu:

```
Unsecured 9860    >
```

```
1.Issue SO Cards
```

2. A prompt will then be displayed:

```
Issue Cards

?
```

   Simply press ENT to acknowledge or CLR to clear.

3. Cards are issued in m of n from 2 of 2 to 9 of 9, Enter ‘n’, the number of cards to be issued between 2 and 9.

```
Num Cards

?
```

4. Enter ‘m’, the number of cards required between 2 and n (selected above).

```
Num Req Cards

?
```

5. If the smart card has not already been entered, it will be prompted for (first 'SO 1' and then each Security Officer smart card in turn until the 'n'th has been entered):

```
Insert Card SO 1

?
```

6. Insert the required smart cards into the smart card reader, entering the Security Officer's actual PIN when prompted. This option is NOT an invitation to give the smart card a new PIN.
7. Remove smart cards when the following prompt appears:

```
Remove Card

?
```

These Security Officer smart cards are tied to the AAK which has been imported (see the next section) or automatically generated if one has not been imported.

The default PIN for a new smart card is set as 11223344. This can be changed when Keyper is in Secured State through the Change PIN menu.

Unsecured State: Restore AAK: Restoring the Authorisation Key from another Keyper

If Security Officer smart cards from another Keyper are to be used then the AAK for those cards needs to be imported.

1. Select Restore AAK option from the Unsecured menu.

```
<Unsecured 9860  >

2.Restore AAK
```

2. Insert the first smart card of the set into the smart card reader when the following prompt appears:

```
Insert Card #1

?
```

3. Remove the smart card when the following prompt is displayed:

```
Remove Card

?
```

4. Insert the next smart card of the set into the smart card reader when the following prompt is displayed:

```
Insert Card #2

?
```

5. Continue the sequence of steps 3 and 4 until AAK Imported is displayed.

Unsecured State: Secure: Switching to Secured State

Switching to Secured State can only be performed once the Security Officer cards have been issued or the AAK imported. A valid set of 'm' Security Officer smart cards are required to successfully execute this operation.

This operation is required to retain the AAK, the Key Export setting, the external SMK algorithm and to secure the Keyper. The Keyper cannot be used for cryptographic purposes unless it is in Secured State.

Do not select this option until sufficient sets of the Security Officer smart cards have been issued.

1. Select Secure from the Unsecured State menu.

```
<Unsecured 9860  >

3.Secure
```

2. Press ENT when the following is displayed:

```
Secure

 ?
```

3. Insert the first Security Officer smart card into the smart card reader, when the following prompt appears:

```
Insert Card SO 1

?
```

4. Enter the smart card PIN when prompted then press ENT. The smart card will then be validated. Remove the smart card when the following prompt appears:

```
Remove Card

?
```

5. In the same manner continue until all 'm' Security Officer smart cards have been presented with their PINs.

6. The next stage is to decide whether to use the Suite B 256bit AES algorithm for backups of Application Keys or the older triple DES algorithm. This choice only affects how keys are exported. Keys may be imported using either AES or triple DES. The default is AES.

```
SMK AES

 Triple DES?
```

7. The next configuration option is to set up the Keyper's port number. This is required to allow the Provider/Load Balancer to communicate with the Keyper. The default is 5000 .Press CLR to decline the invitation to set it up (and accept the default option) or enter the port number. Note that the port number must match the port number configured in the Provider (e.g. the PKCS#11 Provider's machine file) or Load Balancer (as configured in hsm_client.cfg). On completion press ENT. This and the other network settings, may be changed once the Keyper has been secured with the 'HSM Management' menu.

```
Set HSM Port

?
```

```
05000

?
```

8. The next configuration option is to select which IP versions will be used. It is possible to select IPv4 only, IPv6 only or both IPv4 and IPv6. The default is IPv4 and IPv6 which can be selected by pressing CLR. Alternatively use the ‘>’ ‘<’ keys to select the required option and then press the ENT key.

```
V4/V6              >
```

```
1. IPv4 only
```

The next configuration options set the IPv4 network settings if this mode has been selected.

9. The first IPv4 option is to set up the Keyper's IPv4 address. The default is 192.168.0.2 which can be selected by pressing CLR. Alternatively press ENT to enter an address. The address is entered one group of digits at a time. The display prompts for the next group of digits by repeatedly flashing between the default value and “xxx”. To select the default value for a group press the ENT or ‘>’ keys. To select a different value, enter the required digits on the keypad. It is not necessary to enter leading zeroes. If entering less than three digits press the ENT key after entering the digits.

```
Set up IP Addr

?
```

```
192.168.000.002

?
```

```
192.xxx.

?
```

10. The next IPv4 configuration option is to set up the number of bits in the Keyper's net mask. The default is 24 bits, equivalent to a net mask of 255.255.255.0 (i.e. when converted to hex/binary, 255.255.255.0 becomes FF.FF.FF.00, which is a 24 bit mask, counting from the left or most significant end), .Press CLR to decline the invitation to set it up (and accept the default option) or enter the required number of most significant bits in the net mask, between 8 & 32. On completion press ENT.

```
Set Net Mask

?
```

```
24

?
```

11. The final IPv4 network option to be set is the address of the gateway. It is recommended to leave this as all zeroes. Select the default or enter a different address using the same method as setting the IP address.

```
Set Gw Addr

?
```

```
000.000.000.000

?
```

The next three options will only be available if IPv6 has been enabled.

12. The first IPv6 option is to set up the Keyper's IPv6 address. The default is 2001:: followed by fields derived from the unit’s MAC address. Select the default by pressing CLR. Alternatively press ENT to enter an address. The address is entered one group of digits at a time. The display prompts for the next group of digits by repeatedly flashing between the default value and “xxxx”. To select the default value for a group press the ENT or ‘>’ keys. To enter a different value, press the required digits on the keypad. It is not necessary to enter leading zeroes. If entering less than three digits press the ENT key.

```
Set IPv6 address

?
```

```
2001::2e0:6cff:f

Scroll: < >
```

```
2001:xxxx:

?
```

13. The next IPv6 option is to set up the number of bits in the Keyper's IPv6 net mask. The default is 64 bits. Press CLR to accept the default option or enter the required number, between 0 & 128. On completion press ENT.

```
Set IPv6 NetMask

?
```

```
64

?
```

14. The final IPv6 network option to be set is the address of the gateway. The default value is the undefined address “::”. It is recommended to leave this undefined. Select the default with CLR or enter a different address using the same method as setting the IP address.

```
Set IPv6 Gateway

?
```

```
::

Scroll: < >
```

```
2001:xxxx:

?
```

15. The next configuration option is to set up the real time clock. Press CLR to use the current value or ENT to modify the date and time. There is a menu option in Secured State 'HSM Mgmt' menu to change this setting if required.

    Enter the clock in the format as shown below, an error will be displayed if it is incorrectly configured. When the full date/time has been entered press ENT.

```
ddmmyyyyhhmmss

?
```

16. The next option is to insert a configuration smart card. This card holds the Algorithm and API Settings. This will be the profile of the configuration of the standard Keyper in the organisation. It is backed up from the first Keyper configured. If no configuration smart card is to be imported press CLR.

    If a configuration card is to be imported press ENT and enter the configuration smart card when prompted. When prompted enter the PIN associated with the card.

    There are menu options in Secured State menus to change the configuration if required.

```
Import Config

?
```

```
Insert Card

?
```

```
PIN

?
```

17. The next option is to select the FIPS mode. This mode is explained in the Set FIPS Mode section. CLR selects the default of FIPS mode enable. ENT allows the mode to be changed to disabled.

```
FIPS Mode on

 Disable?
```

18. Finally the Keyper displays the global key export state (see the next section). Press ENT or CLR to acknowledge this message. The Key Export state must be set before the unit is secured.

```
Global Key Export

Export Enabled
```

19. The Keyper is now secured and will display the secured menu. However it cannot be used for cryptographic services until the unit is set on-line (see the section on Secured State).

```
Secured  9860-2    >

1.Set Online
```

Unsecured State: Key Export: Setting Key Export Rules

If this option is set to disabled no keys can be backed up or restored by any means whatsoever. Disabling this option overrides all other key export rules.
Once the Keyper has been Secured with key export disabled, this option cannot be reversed without unsecuring the Keyper which will erase all of the keys in the Keyper.

The default is 'enabled'. It is advisable to only disable key export if it is absolutely necessary.

1. Select Key Export from the Unsecured State menu and press ENT to confirm:

```
<Unsecured 9860  >

4.Key Export
```

```
Key Export

?
```

2. Select Disable option by pressing ENT when the following prompt appears:

```
Key Export On

 Disable?
```

Unsecured State: HSM Info: Show Keyper settings and status

1. Select Output Status from the Unsecured State menu and press ENT to confirm:

```
<Unsecured 9860  >
5.HSM Info
```

```
HSM Info
 ?
```

See “Main menu: HSM Info” for further details.

Unsecured State: Identify Cards: Display the card type, version number and serial number of a card

1. Select Output Status from the Unsecured State menu and press ENT to confirm:

```
<Unsecured 9860  >
6. Identify Cards
```

```
Identify Cards
 ?
```

See “Main menu: Identify Cards” for further details.

7 Keyper in Secured State

Keyper is switched to Secured State as described in the section 'Switching to Secured State'.

This is the main menu:

```
Secured 9860-2
1.Set Offline
2.Set Online
3.Set FIPS mode
4.HSM Info
5.Key Mgmt
6.HSM Mgmt
7.Role Mgmt
8.Identify Cards
9.Change PIN
```

The title shows the model number, the 9860 and the variant type, '-2'. Currently this is the only variant supported by the Keyper ^{PLUS}.

Main menu: Set Online: Setting a Keyper Online

Setting a Keyper on-line will allow remote cryptographic operations across the network. Operator smart cards are used to set the Keyper on-line.

1. Select the Set Online from the Main menu.

```
Secured 9860-2    >

1.Set Online
```

2. Insert the first Operator smart card into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card OP 1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. Insert subsequent Operator smart cards in the set, enter the associated PIN, and remove the cards, as prompted.

The READY LED will then be illuminated.

The Keyper will stay on-line until it is reset, powered off or taken off-line (Main menu: Set Offline). When the Keyper powers up, it will remain off-line unless Auto Online is enabled (HSM MgmtL Auto Online).

Main menu: Set Offline: Setting a Keyper Offline

Setting a Keyper off-line will halt all remote cryptographic operations. A set of Operator smart cards perform this function.

1. Select the Set Offline from the Main menu.

```
<Secured  9860-2 >

2.Set Offline
```

2. Insert the first Operator smart card (any card in the set will be accepted) into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card OP 1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. Insert subsequent Operator smart cards in the set, enter the associated PIN, and remove the cards, as prompted.

The READY LED will then go out indicating that the Keyper is off-line.

Main menu: Set FIPS mode: Setting FIPS mode

The Keyper can be set into FIPS or non-FIPS mode. Nearly all applications will either require or can use FIPS mode. In FIPS mode the Keyper only carries out cryptographic operations using FIPS certified algorithms. The only supported non-FIPS certified algorithms are Triple-DES key generation and derivation.

1. Select the Set FIPS Mode from the Main menu:

```
<Secured 9860-2 >
```

```
3.Set FIPS Mode
```

2. Press ENT to acknowledge or CLR to clear:

```
Set FIPS Mode

?
```

3. Insert each Security Officer smart card in a set ('m' cards out of a set of 'n' issued) when prompted and enter the card's PIN:

```
Insert Card SO 1

?
```

4. If all Security Officer smart cards are entered and each card and PIN verified a menu option will be displayed to change the Keyper’s FIPS mode, it will display the text on the left if the Keyper is in FIPS mode and the text on the right if it is in non-FIPS mode. Press ENT to select the mode or CLR to keep the mode unchanged.

```
FIPS Mode On

 Disable?
```

```
FIPS Mode Off

 Enable?
```

Main menu: HSM Info: Show Keyper settings and status

The HSM Info option opens another menu which provides information about the Keyper’s settings and status.

1. First select the HSM Info option and press ENT.

```
<Secured  9860-2 >

4.HSM Info
```

This sub-menu is also available in the HSM Mgmt, Key Mgmt and Role Mgmt menus.

When one of those options has been selected the HSM Info menu becomes available:

```
HSM Info            >

1.Battery Status
---------------------
2.FIPS Mode

3.Time and Date

4.Network

5.S/W Version

6.Serial Number

7.Tamper Counts

8.Output Info
9. Build DateTime
```

HSM Info: Battery Status: View the Keyper's battery status

To determine whether or not the battery is low, simply select the menu option 'Battery Status' from the HSM Info menu:

1 From the HSM Info menu select Battery Status:

```
HSM Info          >

1.Battery Status
```

2 If the battery is OK it will display the following:

```
Battery ok
```

HSM Info: FIPS Mode: Viewing the Keyper's current FIPS mode

To view whether the Keyper is in FIPS mode or non-FIPS mode carry out the following steps.

1. From the HSM Info menu select FIPS Mode:

```
<HSM Info         >

2.FIPS Mode
```

2. If the HSM is in FIPS mode this will be displayed:

```
FIPS Mode On
```

3. If the HSM is not in FIPS mode this will be displayed:

```
FIPS Mode Off
```

4. Press CLR to return to the main menu.

HSM Info: Time and Date: View the Keyper's time and date setting

1. Select Time and Date from the HSM Info menu.

```
<HSM Info        >

3.Time and Date
```

2. Press ENT to view the current time and date.

```
Date dd/mm/yyyy

Time hh:mm:ss
```

Where:

```
dd is the date
mm is the month
yyyyy is the year
hh is the hour
mm is the minutes
ss is the seconds
```

3. Press Enter to confirm

HSM Info: Network: Viewing the Keyper's network configuration

1 Select Network from the HSM Info menu. Press ENT when asked to confirm.

```
<HSM Info        >

4.Network
```

2. Then the Network menu becomes available:

```
Network         >

1.IPv4 Address
-----------------
2.IPv4 Net Mask
3.IPv4 Gway Addr

4.IPv6 Address

5.IPv6 Net Mask
6.IPv6 Gway Addr
7.V4/V6 Enable
8.Port Number
```

Regardless of which v4/v6 modes have been enabled it is always possible to view all the current settings in this menu. These will be the default values if not changed.

IPv4 Address

1. Select IPv4 Address from the Network menu:

```
Network          >

1.IPv4 Address
```

2. The IP address will then be displayed:

```
192.168.0.2
```

IPv4 Net Mask

1. Select IPv4 Net Mask from the Network menu:

```
<Network         >

2.IPv4 Net Mask
```

2. The number of most significant bits in the net mask will then be displayed:

```
24
```

IPv4 Gway Addr

1. Select IPv4 Gway Addr from the Network menu:

```
<Network        >
3.IPv4 Gway Addr
```

2. The address of the gateway will be displayed:

```
0.0.0.0
```

IPv6 Address

1. Select IPv6 Address from the Network menu:

```
<Network              >
4.IPv6 Address
```

2. The IPv6 address will then be displayed:

```
2001::2e0:6cff:f
Scroll: < >
```

The address may be longer than the display so use the '<' and '>' keys to scroll the address to read it all.

IPv6 Net Mask

1. Select IPv6Net Mask from the Network menu:

```
<Network        >
5.IPv6 Net Mask
```

2. The number of most significant bits in the net mask will then be displayed:

```
64
```

IPv6 Gway Addr

1. Select Net Mask from the Network menu:

```
<Network        >
6.IPv6 Gway Addr
```

2. The address of the gateway is shown. If the address is wider than the display use the '<' and '>' keys to scroll through the address. The display below shows the default undefined address.

```
::
Scroll: < >
```

V4 / V6 Enable

1. Select v4/v6 from the Network menu:

```
<Network          >
7. v4/v6 Enable
```

2. The display shows the state of the two protocols:

```
IPV4: disabled
IPV6: enabled
```

Port Number

1. Select Port Number from the Network menu:

```
<Network
8.Port Number
```

2. The port number will then be displayed:

```
05000

?
```

HSM Info: S/W Version: Viewing the Keyper's software version

A Keyper has three different software modules:

Basic Boot Loader (BBL): Responsible for the initial booting of the system and transferring control to the Application Boot Loader.

Application Boot Loader (ABL): Ensures the integrity and authenticity of the Application before launching it. The ABL handles challenge/response for the factory recovery of a positively tampered Keyper

Application (App): The Keyper application and the update handler

The version of the Application also defines the overall Keyper version.

The software version for each of these can be viewed through the S/W Version menu.

1. From the HSM Info menu select S/W Version:

```
<HSM Info          >

5.S/W version
```

2. The version of the BBL is shown:

```
S/W Version        >
 BBL 010
```

3. Use the ‘<’ and ‘>’ keys to scroll through the versions of the other software modules:

```
S/W Version        >
 ABL 011
```

4. Press CLR to return to the Main menu.

HSM Info: Serial Number: View the Keyper's serial number

1. From the HSM Info menu select Serial Number to view the Keyper serial number:

```
<HSM Info           >
6.Serial Number
```

2. The serial number is displayed:

```
Serial Number
```

```
K0101904
```

HSM Info: Tamper Counts: View the number of times a Keyper has tampered

1 From the HSM Info menu select Tamper Counts to view the tamper counts. This option is provided so that owners can provide tamper count information to AEP Networks in the unlikely event that a problem arises.

```
<HSM Info          >
7.Tamper Counts
```

2 Using the > and < keys cycle through the different counts:

```
Tamper Counts    >
  Ext Volt       000
```

```
<Tamper Counts   >
  Int Volt       000
```

```
<Tamper Counts   >
  VBB Volt      000
```

```
<Tamper Counts   >
  Max Temp      000
```

```
<Tamper Counts   >
  Min Temp      000
```

```
<Tamper Counts   >
  Mesh Tamp     000
```

```
<Tamper Counts   >
  Line SMK      000
```

```
<Tamper Counts   >
  Line IMK      000
```

```
<Tamper Counts   >

  Temp Diff      000
```

```
<Tamper Counts   >

  Restart Sw     000
```

```
<Tamper Counts

  Power Fail     000
```

HSM Info: Output Info: Output the Keyper's configuration to the serial port

The unit status can be printed to the serial port. Ensure that a serial cable is connected to a terminal before selecting this menu option.

1. Select Output Status from the Main menu:

```
<HSM Info          >

8.Output Info
```

An example of the print out is shown below. Any items that are not self-explanatory are for the benefit of AEP Networks Support.

```
HSM Status
===================
Keyper 9860
Serial Number K0001288
Date(dd/mm/yyyy) 3/4/2012  Time 14:7:40

Software Versions:
BBL 010               ABL 010               App 010


CPLD Version:
1.9



Memory Usage:
RAM (free/total)      202Mb/256Mb
Flash (free/total)    127Mb/128Mb
   black store                              276b
   statistics                               168b
   other                                    116b
RedStore (free/total) 109Kb/128Kb

Network Configuration:
Factory MAC/IP address: 00:E0:06:C0:00:FF / 192.168.0.2/24
HSM Port 05000
HSM Gateway 0000.
tsec0: flags=8a43<UP,BROADCAST,RUNNING,ALLMULTI,SIMPLEX,MULTICAST> mtu 1500
                      capabilities rx=7<IP4CSUM,TCP4CSUM,UDP4CSUM>
                      capabilities tx=0
                      enabled=0
                      address: 00:e0:06:c0:00:ff
                      media: Ethernet autoselect (100baseTX full-duplex)
                      status: active
                      inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
```

```
Current HSM State: Managed

Modes: (1=Enabled 0=Disabled)
Global Key Export    1App Key Import      1App Key Export      1Asymmetric Key Gen    1
Symmetric Key Gen    1Symmetric Key Derive 1Signing              1Signature Verify      1
MAC Generation       1MAC Verification     1Encrypt / Decrypt    1Delete Asym Key       1
Delete Sym Key       1Output Key Details   1Output Key Summary   1Suite B Algorithms    1
Non Suite B Algs     1Auto Online          0
Other Modes:
AES SMK               FIPS Mode

Battery ok

####################################
###     ABL tamper records       ###
####################################
Current Tamper Counts (decimal 0-255):
======================================
vextoosTamperCount:   0
vintoosTamperCount:   0
vbboosTamperCount:    0
maxstrtempTamperCount:0
minstrtempTamperCount:0
meshTamperCount:      0
extampSMKTamperCount: 0
extampIMKTamperCount: 0
tempdiffTamperCount:  0
pfTamperCount:        0
restartTamperCount:   0

Current tamper bitmaps:
=======================
currentTamper bitmap: 0x0000 0b .... .... .... ....
```

```
lastTamper bitmap:    0x0000 0b .... .... .... ....

Bitmapped Change Record (most recent first):
============================================
5: 0x0040 0b .... .... .1.. ....  |EXTAMP_IMK
4: 0x0040 0b .... .... .1.. ....  |EXTAMP_IMK
3: 0x0040 0b .... .... .1.. ....  |EXTAMP_IMK
2: 0x0040 0b .... .... .1.. ....  |EXTAMP_IMK
1: 0x0008 0b .... .... .... 1...  |MESH
```

Selecting this menu option also causes the DRBG to execute a self-test.

HSM Info: Build DateTime: Get the application build details

1. From the HSM Info menu select Serial Number to view the Keyper serial number:

```
<HSM Info
9.Build DateTime
```

2. The date and time that the Keyper application was built are shown. This provides additional information to AEP Networks Support:

```
10:43:47
 Nov  6 2012
```

Main menu: Key Mgmt: Key Management

A set of Crypto Officers are required to access the Key Management functions.

1. First select the Key Mgmt menu and press ENT:

```
<Secured  9860-2 >

5.Key Mgmt
```

2. Insert the first CO smart card into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card CO 1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. Insert subsequent CO cards into the smart card reader, enter their associated PINs and remove the cards as prompted.

Then the Key Management menu becomes available:

```
Key Mgmt          >

1.Key Summary
```

```
2.Key Details

3.App Keys

4.SMK

5.API Settings

6.Alg Settings

7.Config

8.HSM Info
```

Key Mgmt: Key Summary

This option outputs a summary of the keys held in the Keyper's key store via the serial port.

1. Select Key Summary from the Key Mgmt menu:

```
 Key Mgmt        >

1.Key Summary
```

2. At the prompt, select ENT to confirm the operation.
3. A summary of the keys held in the Keyper's key store is output via the serial port:

```
Dumping HSM Key Summary
=======================


RSA,4096,Private,5
```

```
AES,0128,,1
TDES,0168,,5
==================
```

The format is:

<key type>,<key size>,<public or private or neither>,<number of keys matching the description>

So the example above shows that there are 5 x private RSA 4096 bit keys, 1 x 128 bit AES key and 5 x 168 bit triple DES keys stored in the Keyper.

Key Mgmt: Key Details

This option outputs details of each of the keys held in the Keyper's key store via the serial port.

1. Select Key Details from the Key Mgmt menu:

```
<Key Mgmt        >
2.Key Details
```

2. At the prompt, select ENT to confirm the operation.
3. A detailed list of the keys held in the Keyper's key store is output via the serial port:

```
Dumping HSM Key Details
========================
privRSA,RSA,FIPS,4096,wt,svedmvu
privRSA,RSA,FIPS,4096,wt,svedmvu
aes128,AES,FIPS,0128,wt,sedmvwu
CKSLOT,TDES,Non-FIPS,0168,wt,svedmvwu
CKSLOT,TDES,FIPS,0168,wt,svedmvwu
CKSLOT,TDES,FIPS,0168,wt,svedmvwu
CKSLOT,TDES,FIPS,0168,wt,svedmvwu
CKSLOT,TDES,FIPS,0168,wt,svedmvwu
privRSA,RSA,FIPS,4096,wt,svedmvu
privRSA,RSA,FIPS,4096,wt,svedmvu
privRSA,RSA,FIPS,4096,wt,svedmvu
==================
```

The format is:

<key label>,<key type>,<FIPS or non-FIPS key>,<key size>,<key policy><key usage>

<key label>: the key label is the first 7 characters of the PKCS#11 label as set when the key was generated/imported. If it was not set or PKCS#11 was not used to generate or import the key it is set to 'CKSLOT'.

<key policy> options:

p – key can be exported in plain text

w – key can only be exported wrapped by another key

v – key has a fixed IV (triple DES)

t – key is a token key

<key usage> options:

s – key can sign (ECDSA, RSA only)

v – key can verify signatures (ECDSA, RSA only) e – key can encrypt data

d – key can decrypt data

m – key can MAC (Triple DES, AES only)

v – key can verify MACs (Triple DES, AES only)

u – key can unwrap other keys

w – key can wrap other keys

Key Mgmt: App Keys: Managing Application Keys

Application Keys are keys generated by a request for cryptographic services, e.g. a key generation request by a host. An example of an Application Key is a CA root-signing key.

Application keys are protected by the ISMK while stored within the Keyper. The keys are wrapped by the SMK for backup and restore. Protected keys consist of key material, the key policy and a key identifier.

Application Keys cannot be backed up or imported if Key Export rules are set to off.

1. First select App Keys from the Key Mgmt menu:

<Key Mgmt	>
3.App Keys	

Then the App Key menu becomes available:

App Keys	>
1.Backup	
2.Restore	

3.Legacy Backup

4.Legacy Restore

5.Clear Media

6.Media Contents

7.Erase App Key

Application Key Backup and Restore

The following sections describe the four menu options to back-up and restore Application keys.

One pair of options, ‘1. Backup’ and '2.Restore', are used for transferring keys to and from Keypers of type 9720 version 1.7 and later.

The other options, ‘3. Legacy Backup’ and'4.Legacy Restore', are used for transferring keys to and from Keypers of type 9720 version 1.6. This menu option only works with the pre-printed 128k Application Key smart cards.

Keyper Model 9720 version 1.8 and earlier only support TDES SMKs.

USB can only be used with Keyper ^{PLUS}.

DES keys whose length is less than 112 bits cannot be imported into the Keyper ^{PLUS}.

The following table summarises the valid options when backing-up / restoring Application Keys to older version of Keyper.

Target Keyper	SMK Type	Media	Menu Selections
9860	AES / TDES	Smart Card / USB	1. Backup / 2. Restore
9720 version 1.9 – 2.0	AES / TDES	Smart Card	1. Backup / 2. Restore
9720 version 1.7 – 1.8	TDES	Smart Card	1. Backup / 2. Restore
9720 version 1.6 and earlier	TDES	Smart Card	3. Legacy Backup / 4. Legacy Restore

These option are not available if Key Export is disabled while the Keyper is being Secured.

Before backing-up keys ensure the current SMK has been backed-up.

Before performing any of these operations the Keyper must be off-line.

Several menu operations involve selecting keys from a list. The user interface behaves the same in each case. The display shows the labels for two keys, one on each line.

The ‘<’ and ‘>’ keys can be used to scroll the list of keys up and down. Keys preceded with an ‘*’ are currently selected. Keys preceded with a space are not currently selected.

The ‘A’ and ‘D’ keys can be used to select and un-select the top key on the display. Pressing the ‘A’ key will select the key and it will be marked with a ‘*’. Pressing the ‘D’ key will de-select the key and it will be marked with a space.

Once all the required keys have been selected pressing the ENT key will cause the current menu operation to be performed on all the selected keys.

Key Mgmt: App Keys: Backup: Backing up all Application Keys to USB memory sticks

1. Select Backup:

```
 App Keys          >

1.Backup
```

2. Select the media to back-up to:

```
Which Media?      >

1.Backup to USB
```

3. Select All Keys:

```
USB               >

1.All Keys
```

4. Confirm the selected keys are to be backed up (All Keys) by pressing ENT (at this point keys can be deselected (shown by a *) by scrolling up or down the list using the '<' and '>' keys, and then pressing 'D' to clear or 'A' to add the entry on the top line):

```
  <Key Id>

  <Key Id>
```

5. Insert the USB memory stick. Confirm by pressing ENT. Note that only one will be prompted for. A single memory stick is sufficient to hold the entire key store. It must be a supported USB memory stick with a FAT 16 or FAT 32 filesystem (see Appendices).

```
Insert USB

?
```

6. When complete, the message *Done* is displayed.

Key Mgmt: App Keys: Backup: Backing up all Application Keys to Cards (any size)

1. Select Backup:

```
App Keys          >

1.Backup
```

2. Select the media to backup to:

```
<Which Media?

2.Backup to Card
```

3. Select All Keys:

```
 Smartcard        >

1.All Keys
```

4. Confirm the selected keys are to be backed up (All Keys) by pressing ENT (at this point keys can be deselected by scrolling up or down the list using the '<' and '>' keys, and then pressing 'D' to clear or 'A' to add the entry on the top line):

```
* <Key Id>
* <Key Id>
```

5. Insert the first Application Key smart card. Confirm by pressing ENT.

```
Insert B/U Card

?
```

6. Insert the next smart card at the following prompt. Continue in this manner until the backup has been completed.

```
Insert B/U Card

?
```

7. When complete, the message *Done* is displayed.

Key Mgmt: App Keys: Backup: Backing up selected Application Keys to Cards (any size)

1. Select Backup:

```
App Keys           >

1.Backup
```

2. Select the media to backup to:

```
<Which Media?     >

2.Backup to Card
```

3. Select Specify key:

```
<Smartcard

2.Specify key
```

4. Select the keys to back-up using the instructions in the Application Key Backup and Restore section.

```
* <Key Id>

  <Key Id>
```

5. Insert the first Application Key smart card. Confirm by pressing ENT.

```
Insert B/U Card

?
```

6. Insert the next smart card at the following prompt. Continue in this manner until the backup has been completed.

```
Insert B/U Card

?
```

7. When complete, the message Done is displayed.

Key Mgmt: App Keys: Restore: Restoring Application Keys

This menu option for Application Key restoration, '2.Restore' allows the import of Application Keys on smart card or USB memory stick.

1. Select Restore

```
<App Keys          >
2.Restore
```

2. Select the media to restore from (in this example USB):

```
<Which Media?
2.Restore from USB
```

3. When complete, the message Done will be displayed.

Key Mgmt: App Keys: Legacy Backup

1. Select Legacy Backup:

```
<App Keys          >
3.Legacy Backup
```

2. Select the keys to back-up using the instructions in the Application Key Backup and Restore section..

```
* <Key Id>
* <Key Id>
```

3. Insert the first Application Key smart card and confirm by pressing ENT.

```
Insert Card #1

?
```

4. Insert the next smart card at the following prompt. Continue in this manner until the backup has been completed (i.e. #2, then #3 etc).

```
Insert Card #2

?
```

5. When complete, the message 'Done' will be displayed.

Key Mgmt: App Keys: Legacy Restore: Restoring Application Keys from a smart card

1. Select Legacy Restore.

```
<App Keys          >

4.Legacy Restore
```

2. Insert the first Application Key smart card. Confirm by pressing ENT.

```
Insert Card #1

?
```

3. Insert the next smart card at the following prompt. Continue in this manner until the backup has been imported (i.e. #2, then #3 etc).

```
Insert Card #2

?
```

4. When complete, the message Done will be displayed.

Key Mgmt: App Keys: Clear media: Erase Application key from a USB memory stick

Clearing a USB memory stick will remove all keys currently saved on it.

1. Select Clear Media:

```
<App Keys          >

5.Clear Media
```

2. Select the media to erase:

```
Which Media?      >

1.Clear USB
```

3. Insert the Application Key USB memory stick to be cleared.

```
Insert USB

?
```

Key Mgmt: App Keys: Clear media: Erase Application keys from a smart card

Clearing a smart card will remove all information currently saved on it and will leave the smart card "blank". This option can only be used to clear/format non-legacy application key backup smart cards.

1. Select Clear Media:

```
<App Keys          >

5.Clear Media
```

2. Select the media to erase:

```
<Which Media?

2.Clear Card
```

3. Insert the Application Key smart card to be cleared.

```
Insert Card #1

?
```

4. Remove the smart card when prompted.

Key Mgmt: App Keys: Media contents: Output Application Key details from USB memory stick

This menu option outputs a list of all Application Keys stored on a USB memory stick to the serial port.

1. Select Media Contents from the App Keys menu:

```
<App Keys          >
6.Media Contents
```

2. Select the media to be viewed:

```
Which Media?      >
1.View USB
```

3. Insert the Application Key USB memory stick to be viewed.

```
Insert USB
?
```

4. Select ENT to continue.
5. The Keyper prompts to allow details to be output to the serial port:

```
View Details
?
```

6. Press ENT to confirm or CLR to decline.
7. The application key details are output via the serial port.
8. Remove the USB memory stick when prompted.

Key Mgmt: App Keys: Media contents: Output smart card Application key details from smart card

This menu option outputs a list of all Application Keys stored on a smart card to the serial port.

1. Select Media Contents from the App Keys menu:

```
<App Keys         >
6.Media Contents
```

2. Select the media to be viewed:

```
<Which Media?
2.View Card
```

3. Insert the Application Key smart card to be viewed.

```
Insert Card #1
?
```

4. The media type and serial number are shown on the display
5. Select ENT to continue
6. The Keyper prompts to allow details to be output to the serial port:

```
View Details
?
```

7. Press ENT to confirm or CLR to decline.

8. The application key details are output via the serial port.
9. Remove the smart card when prompted.
10. The Keyper prompts for Another Card?:

Key Mgmt: App Keys: Erase App Keys: Erasing Application keys from the Keyper

This menu option erases all Application Keys stored inside the Keyper.

1. Select Erase App Keys from the App Keys menu:

```
<App Keys

7.Erase App Keys
```

2. At the prompt, select ENT to confirm application key deletion.

```
Erase App Keys

?
```

3. Select either option 1 to delete all keys or option 2 to select specific keys to delete.

```
Erase App Keys    >

1. All Keys
```

4. Select the keys to erase using the instructions in the Application Key Backup and Restore section. Press ENT to delete the selected keys.

Key Mgmt: SMK: Managing the Storage Master Key (SMK)

The Storage Master Key (SMK) is used to wrap the Application Keys. It can be backed up or restored in component form

Two SMKs are supported; a 256 bit AES SMK and a 168 bit triple DES SMK. Both SMKs can be imported and used to unwrap imported application keys. Only the algorithm type selected during the Securing procedure can be generated or exported. The default SMK algorithm is 256 bit AES.

No SMK options are available if Key Export is disabled while the Keyper is being Secured.

1. First select SMK from the Key Mgmt menu:

```
<Key Mgmt        >
4.SMK
```

2. Then the SMK menu becomes available:

```
SMK              >
1.Generate SMK
-----------------
2.Backup SMK
3.Restore SMK
4.Clear Cards
5.View Cards
```

Key Mgmt: SMK: Generate SMK: Generating a Storage Master Key (SMK)

This option generates a new SMK. Its algorithm is the one selected during the Securing procedure.

1. Select Generate from the SMK menu:

```
SMK               >

1.Generate SMK
```

2. When the operation has completed the following message appears.

```
SMK Generated
```

3. Press ENT to return to the main menu.

If Keyper is set to Key Export rules on, 'ACCESS DENIED' is displayed.

Key Mgmt: SMK: Backup SMK: Backing up a Storage Master Key (SMK)

1. Select Backup SMK from the SMK menu:

```
<SMK              >

2.Backup SMK
```

2. Enter the number of components the SMK is to be exported in, between 4 and 9.

```
Num Cards

?
```

3. The following prompt will then be displayed. The number of smart cards required for further imports would be between 2 and the number of smart cards specified at the Num Cards? prompt.

```
Num Req Cards

?
```

1. Keyper displays the prompt Insert Card and then for the Next Card until the number of smart cards specified have been formatted. Press ENT to confirm the smart card clear or press CLR to return to the previous menu.
2. Insert the first SMK smart card at the following prompt.

```
Insert Card #1

?
```

1. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

Insert the next SMK smart card. Continue until the SMK has been exported.The export of the SMK will then be tested by re-inserting each of the cards when prompted:

```
Verify Card #1

?
```

1. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

2. Continue re-inserting cards as prompted until the following message is displayed:

```
SMK Backed Up
```

The SMK has now been successfully backed-up and it has been verified that it can be recreated from each combination of m from n cards.

If Keyper is set to Key Export rules on, ACCESS DENIED is displayed.

Key Mgmt: SMK: Restore SMK: Restoring a Storage Master Key (SMK)

This option allows the SMK to be imported into the Keyper from smart cards.

1. Select Restore SMK from the SMK menu:

```
<SMK           >

3.Restore SMK
```

2. Insert a smart card into the smart card reader when the following prompt appears:

```
Insert Card SMK 1

?
```

3. Insert the next smart card of the set and continue until all the components have been imported.

```
Insert Card #2

?
```

4. When the operation has completed the following message appears. Press ENT to return to the main menu.

```
SMK Restored
```

If Keyper is set to Key Export rules on, ACCESS DENIED is displayed.

Key Mgmt: SMK: Clear Cards: Clearing a Storage Master Key (SMK) smart card

Clearing a smart card will remove all information currently saved on it and will leave the SMK smart card "blank". Each smart card submitted for clearing must be an SMK smart card.

1. Select Clear Card from the SMK menu:

```
<SMK

4.Clear Cards
```

2. Insert the first SMK smart card to be cleared when the following prompt appears:

```
Insert Card SMK1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. The following message will be displayed:

```
SMK Cleared
```

Key Mgmt: SMK: View Cards: Display the card type, version number and serial number of a card

To view (any) smart card properties:

1. Select Identify Cards from the SMK menu:

```
<SMK

5.View Cards
```

2. Insert the smart card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. The smart card type and serial number are displayed (example below):

```
SMK v1

ssssssssssssssssss
```

4. The Keyper prompts to allow card details to be output:

```
Output Details

?
```

5. Selecting ENT will cause the card details to be output via the serial port. Selecting CLR skips this output.

Key Mgmt: API Settings: Enabling/Disabling Selected API Operations

These menu options allow different API operation to be enabled or disabled. The default setting is all options enabled.

If Keyper is set to Key Export disabled (when the Keyper is Secured), the Key Export and Key Import options are ignored.

The API Settings menu allows the following operations to be disabled/enabled:

- Key Import
- Key Export
- Asymmetric Key Generation (ECDSA, DSA, RSA only)
- Symmetric Key Generation (AES, triple DES only)
- Symmetric Key Derivation (AES, triple DES only)
- Signing (ECDSA, RSA only)
- Verifying Signatures (ECDSA, RSA only)
- MAC Generation (AES, triple DES only)
- MAC Verification (AES, triple DES only)
- Encryption/Decryption
- Asymmetric Key Deletion (ECDSA, DSA, RSA only)
- Symmetric Key Deletion (AES, triple DES only)

1. Select API Settings from the Key Mgmt menu

```
<Key Mgmt        >
5.API Settings
```

Then the API Settings becomes available:

```
API Settings     >
1.Key Import
2.Key Export
```

```
3.Asym Key Gen
4.Sym Key Gen
5.Sym Key Der
6.Signing
7.Verifying
8.MAC Gen
9.MAC Ver
A.Enc/Dec
B.Asym Key Del
C.Sym Key Del
```

2. Select the option to change (e.g. 2.Key Export):

```
<API Settings       >
2.Key Export
```

3. If Key Export is currently enabled, the following menu will be displayed:

```
Key Export On
 Disable?
```

4. To disable Key Export press ENT. To leave Key Export enabled press CLR and return back to the Key Mgmt menu.
5. The action is audited.

The other API settings can be changed in a similar way..

Key Mgmt: Alg Settings: Enabling Algorithm Suite B and Non-Suite B

The Alg Settings menu allows the following sets of algorithms to be disabled / enabled:

Suite B algorithms (AES, ECDH & ECDSA) are always enabled. In addition, Non-Suite B algorithms (TDES, DSA and RSA) can be enabled or disabled

1. Select Alg Settings from the Key Mgmt menu

```
<Key Mgmt        >
6.Alg Settings
```

2. If Suite B only is currently enabled the following will be displayed:

```
SuiteB Only On
 Disable?
```

Select ENT to disable the mode or CLR to leave it enabled.

3. If Suite B only is currently disabled the following will be displayed:

```
SuiteB Only Off
 Enable?
```

Select ENT to enable the mode or CLR to leave it disabled.

4. The action is audited.

Key Mgmt: Config: Backup and Restore API and Alg Settings

The Config function allows the Keyper's API and Alg settings (see API Settings and Alg Settings) to be exported from a Keyper and then either kept as a backup and/or imported into another Keyper. This allows a set of Keyper's to maintain the same profile.

Config smart cards are protected by a PIN that has to be entered on export and to be entered before an import is accepted.

1. Select Config from the Key Mgmt menu:

<Key Mgmt > 7.Config

The following menu will then become available:

Config > 1.Import Config.
2.Export Config. 3.Clear Cards 4.View Cards

Key Mgmt: Config: Import: Import API and Alg Settings from smart card

The Import Config option allows a set of configuration parameters to be loaded from smart card. The configuration variables include the API Settings and Algorithm Settings variables.

1. Select Import from the Config menu:

```
Config              >

1.Import Config.
```

2. Enter a configuration smart card into the smart card reader and the PIN when prompted and the configuration variables will be imported from it. Remove the card when prompted.

Key Mgmt: Config: Export: Export API and Alg Settings onto a smart card

The Export Config option allows the current set of configuration parameters to be backed up onto smart card. The configuration variables include the API Settings and Algorithm Settings variables.

1. Select Export from the Config menu:

```
<Config             >

2.Export Config.
```

2. Enter a configuration smart card into the smart card reader when prompted and then the existing PIN (the default on a new card is 11223344) and the configuration variables will be exported to it. Remove the card when prompted.

Key Mgmt: Config: Clear Config Card: Erase all of the contents from a Config card

To clear any Configuration card:

1. Select Clear Cards from the Config menu:

```
<Config

3.Clear Cards
```

2. Insert the card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. Remove the smart card when prompted.

Key Mgmt: Config: Identify Card: Display the card type, version number and serial number of a card

To view (any) smart card properties:

1. Select Identify Cards from the Config menu:

```
<Config

4.View Card
```

2. Insert the smart card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. The smart card type and serial number are displayed (example below):

```
Config Card v1

ssssssssssssssssss
```

4. The Keyper prompts to allow card details to be output:

```
Output Details

?
```

5. Selecting ENT will cause the card details to be output via the serial port. Selecting CLR skips this output.

Key Mgmt: HSM Info: Show Keyper settings and status

1. First select the HSM Info menu:

```
<Key Mgmt

8.HSM Info
```

This will make the HSM Info menu available. See section Main menu: HSM Info for details.

Main menu: HSM Mgmt: HSM Management

A set of Security Officers are required to access the HSM Management functions.

1. First select the HSM Mgmt menu:

```
<Secured  9860-2 >

6.HSM Mgmt
```

2. Insert the first SO smart card into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card SO 1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. Insert subsequent Security Officer cards into the smart card reader, enter their associated PINs and remove the cards as prompted.
5. This following HSM Management menu then becomes available:

```
HSM Mgmt          >

1.Auto Online
```

```
2.Change Clock

3.Set Network

4.View Cards

5.Unsecure

6.Statistics

7.HSM Info
```

Selecting and then existing a sub-menu returns to this menu unless a key has not been pressed within 10 minutes.

HSM Mgmt: Auto Online: Allows the unit to not change state over power cycle

When Auto Online is enabled a Keyper will automatically go on-line when it is powered-up if the Keyper was on-line when it was powered off. When Auto Online is disabled the Keyper will remain off-line until it is taken on-line by an Operator (see Main menu: On line).

1. Select Auto Online from the HSM Mgmt menu and press ENT:

```
HSM Mgmt        >

1.Auto Online
```

2. The current state is displayed, in this case disabled (off). Press ENT to change the state, in this case to enabled or press CLR to leave the state unchanged.

```
Auto Online Off

 Enable?
```

HSM Mgmt: Change Clock: Changing the Real Time clock

1. Select Change Clock from the HSM Mgmt menu:

```
<HSM Mgmt        >
2.Change Clock
```

2. See HSM Info: Time and Date for details of setting the time and date.

HSM Mgmt: Set Network

The Edit Network menu allows the network configuration to be set up (see Section 8 for usage).

1. First select Set Network from the HSM Mgmt menu:

```
<HSM Mgmt        >
3. Set Network
```

2. The following network menu will then be available:

```
Set Network        >
1.IPv4 Address
2.IPv4 Net Mask
3.IPv4 Gway Addr
4.IPv6 Address
5. IPv6 Net Mask
6. IPv6 Gway Addr
7. V4/V6 Enable
8. Port  Number
```

Select the item to change using the ‘<’, ‘>’ keys and press ENT. Refer to Unsecured State: Secure: Switching to Secured State for details on how to modify each field.

HSM Mgmt: Identify Cards: Display the type, serial no. and smart card version

To view smart card properties:

1. Select Identify Cards from the Config menu:

```
<HSM Mgmt          >
4.View Cards
```

2. Insert the smart card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. The smart card type and serial number are displayed (example below):

```
SO v1

ssssssssssssssss
```

(where ssssssssssssssss is the serial number)

4. The Keyper prompts to allow card details to be output:

```
Output Details

?
```

5. Selecting ENT will cause the card details to be output via the serial port. Selecting CLR skips this output.

HSM Mgmt: Unsecure

This menu option will return the Keyper to ‘Unsecured’ state as if it were just shipped from AEP Networks. This will erase all keys, API settings, Alg settings and the network configuration. It will also invalidate all Operator, Security Officer and Crypto Officer smart cards that were issued unless the AAK has been backed-up.

IMPORTANT: *Network Services must have been stopped before this operation. Otherwise an ACCESS DENIED error message will be displayed.*

It may take a few minutes for Keyper to restart after erasing all keys.

1. Select ‘Unsecure’ from the HSM Mgmt menu:

```
<HSM Mgmt        >
5.Unsecure
```

2. Confirm the state change by pressing ENT (or reject by pressing CLR).

WARNING: *This action will clear all the keys, including the SMK and AAK, and reset the networks settings and other configuration options.*

When this operation is complete the Keyper will reboot into the 'Unsecured State'.

HSM Mgmt: Statistics

1. Select the Statistics option:

```
<HSM Mgmt        >
6.Statistics
```

2. When prompted to press enter to confirm the selection:

```
Statistics

?
```

The Keyper statistics will be output on the serial port.

The start of the report gives the time the time the HSM was powered up and the time the unit went operational (on-line). The values are also displayed from the previous time the unit powered-up and went operational.

```
                 API CALL SUMMARY @ Mon Mar 12 15:00:08 2012

               Current HSM power up/operational time
HSM power up time    : Mon Mar 12 11:15:20 2012
HSM operational time: Mon Mar 12 11:15:21 2012

               Prev HSM power up/operational time
HSM power up time    : Fri Mar  9 16:52:21 2012
HSM operational time: Fri Mar  6 16:52:23 2012
```

There is a summary for each algorithm and key length which shows the minimum, maximum and average execution times for all requests, the total number of requests and a breakdown by type of operation.

For example, the following sample shows the time taken for 55 ECDSA 192 requests consisting of 32 sign operations and 23 verify operations.

```
Algorithm:ECC Mech:ECDSA KeyLength:192
min time:3 ms
max time:16 ms
average time:6 ms
incoming requests:55
 - counter:sign  calls:32
 - counter:verify  calls:23
```

HSM Mgmt: HSM Info: Show Keyper settings and status

1. First select the HSM Info menu:

```
<HSM Mgmt
7.HSM Info
```

This will make the HSM Info menu available. See section Main menu: HSM Info for details.

Main menu: Role Mgmt: Role Management

Role cards protect against unauthorised access by providing the means to authenticate users. The Role Management menu allows a Security Officer to issue, view and clear Role cards.

Each role card is authenticated using the AAK key. To authenticate a Role Card, the Keyper must contain the same AAK as when the card was issued.

Role cards can be managed across a group of Keypers by using the same AAK on each Keyper. The AAK is generated by one Keyper, exported and then imported into other Keypers.

The AAK is restored while Keyper is in the 'Unsecured State' and backed up while in 'Secured State'. See the section on the Keyper in Unsecured State for details on how to restore the AAK.

Note: Disabling Key Export has no effect on issuing Crypto Officer and Operator smart cards.

A set of Security Officers are required to access the Role Management functions.

1. First select the Role Mgmt menu:

```
<Secured  9860-2 >

7.Role Mgmt
```

2. Insert the first SO smart card into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card SO 1

?
```

3. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

4. Insert subsequent SO cards into the smart card reader, enter their associated PINs and remove the cards as prompted.

The Role Management menu then becomes available:

```
Role Mgmt          >
1.Issue Cards
2.View Cards
3.Backup AAK
4.Clear RoleCard
5.Clear AAK Card
6.HSM Info
```

Role Mgmt: Issue Cards: Issuing Crypto Officer or Operator smart cards

This option allows a set of Crypto Officer or Operator cards to be issued.

1. Select Issue Cards from the Role Mgmt menu:

```
Role Mgmt         >
1.Issue Cards
```

2. Then press ENT.

```
Issue Cards
?
```

3. Select the card type to issue either Crypto Officer or Operator

```
Issue Cards        >

1.Issue CO Cards
```

```
<Issue Cards

2.Issue OP Cards
```

4. The Keyper prompts for the number of cards in the set to be entered: Num Cards?
5. Enter the number of cards in the set.
6. The Keyper prompts for the number of cards required to authorise an operation to be entered: Num Req Cards?
7. Enter the number of cards required to authorise an operation.
8. When prompted insert blank CO cards:

```
Insert Card #1

?
```

9. Insert the next smart card and press ENT until all the smart cards have been issued.

```
Insert Card #2

?
```

The cards must be formatted Crypto Officer / Operator smart cards or brand new smart cards.

Role Mgmt: View Cards: Display the card type, version number and serial number of a card

To view smart card properties:

1. Select View Cards from the Role Mgmt menu:

```
<Role Mgmt        >

2. View Cards
```

2. Insert a smart card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. The smart card type and serial number are displayed

```
CO v1

ssssssssssssssss
```

where ssssssssssssssss is the serial number.

4. The Keyper prompts to allow card details to be output:

```
Output Details
```

```
?
```

5. Selecting ENT will cause the card details to be output via the serial port. Selecting CLR skips this output.

Role Mgmt: Backup AAK: Backing up the Authorisation Key (AAK) to smart card

The AAK can be backed up at any time while Keyper is in 'Secured State'.

1. Select Back AAK from the Role Mgmt menu:

```
<Role Mgmt        >

3.Backup AAK
```

2. Enter the number of components, between 2 and 9, in which to export the AAK:

```
Num cards

?
```

3. Insert the first smart card at the following prompt:

```
Insert Card #1

?
```

4. Remove the smart card from the smart card reader, when the following prompt appears:

```
Remove Card

?
```

5. Repeat these steps for all subsequent cards (prompts for #2, #3 etc) until all components have been backed up and AAK Exported is displayed.

Role Mgmt: Clear Role Cards: Clearing Operator, Security Officer and Crypto Officer smart cards

Clearing a smart card will remove all information currently saved on it and will leave the smart card "blank".

1. Select Clear Card from the Role Mgmt menu :

```
<Role Mgmt        >

4.Clear Role Card
```

2. Insert the smart card to be cleared into the smart card reader. Confirm by pressing ENT and enter the PIN.

```
Insert Card #1

?
```

3. Insert the next smart card and press ENT until all the required smart cards have been cleared.

Role Mgmt: Clear AAK Cards: Clearing AAK smart cards

Clearing a smart card will remove all information currently saved on it and will leave the smart card "blank".

1. Select Clear Card from the Role Mgmt menu :

```
<Role Mgmt        >

5.Clear AAK Card
```

2. Insert the smart card to be cleared into the smart card reader.

```
Insert Card #1

?
```

3. Insert the next smart card and press ENT until all the required smart cards have been cleared.

4. Enter the number of smarts cards to clear, a maximum of 9. Confirm by pressing ENT.

```
Num cards

?
```

5. Insert the smart card to be cleared at the following prompt:

```
Insert Card AAK1
```

```
?
```

6. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

7. Keyper will then prompt for the Next Card (AAK2 etc) until the number of smart cards specified has been cleared.

Role Mgmt: HSM Info: Show Keyper settings and status

1. First select the HSM Info menu:

```
<Role Mgmt

6.HSM Info
```

This will make the HSM Info menu available. See section Main menu: HSM Info for details.

Main menu: View Cards: Display the type, serial no and version of a smart card

This menu provides generic information about any type of smart card. More specific information can be obtained by using the View Card option within the sub-menu where the card was issued. For example, under the HSM Mgmt menu, the View Card option will list all the API settings held on the card.

To view the properties of a card:

1. Select Identify Cards from the SMK menu:

```
<Secured  9860-2  >

8.View Cards
```

2. Insert the smart card into the smart card reader when the following prompt appears.

```
Insert Card

?
```

3. The smart card type and serial number are displayed (example below):

```
SMK v1

ssssssssssssssssss
```

4. The Keyper prompts to allow card details to be output:

```
Output Details

?
```

5. Selecting ENT will cause the card details to be output via the serial port. Selecting CLR skips this output.

These are examples of what is displayed when a card is viewed.

The display below shows that the card is a current Operator Officer smart card:

```
OP v1

00C000000DF20DF7
```

The display below shows that the card is a current Security Officer smart card:

```
SO v1

00C000000DF20E65
```

The display below shows that the card is a current Crypto Officer smart card:

```
CO v1

00C000000DF29E65
```

The display below shows that the card is a SMK component smart card, if ENT is then pressed it shows the card manufacturer and pressing ENT again gives the manufacturers card model:

```
SMK v0

0200000198970E65
```

```
Manufacturer:

GemPlus
```

```
Product:

MPCOS EMV
```

```
Card size:

16 kbits
```

The display below shows that the card is an Application Key smart card version 2 format:

```
App v2

018000001FB20E65
```

The display below shows that the card is an original AAK smart card (the format has not changed since the Zergo HSP4000 HSM that preceded the AEP Networks Keyper range):

```
AAK v0

0140000001F20E65
```

The display below shows that the card is not an AEP Networks Keyper smart card. Either it is unformatted or it has been formatted by another product:

```
Invalid File

Error 9006
```

1. When ready, press ENT. The display then presents the option to read another smart card's type. Press CLR to exit or ENT and then enter the smart card to be read when prompted.

```
Another Card?

?
```

Main menu: Change PIN: Changing the smart card PIN

A smart card with an associated PIN (i.e. an Operator, Security Officer, Crypto Officer or Configuration smart card) is issued for the first time with the default PIN 11223344. To change it do the following:

1. Select Change PIN from the Main menu.

```
<Secured 9860-2
9.Change PIN
```

2. Enter the smart card into the smart card reader when the following prompt appears:

```
Insert Card
?
```

3. Enter the old PIN. The default PIN is 11223344. Confirm by pressing ENT:

```
Old PIN
?
```

4. Enter the new PIN and press ENT:

```
PIN
?
```

5. Confirm the new PIN by entering it again and pressing ENT. The new PIN is now set.

```
Confirm

?
```

6. Remove the smart card from the smart card reader when the following prompt appears:

```
Remove Card

?
```

8 Recovering from a Tamper

When a positive tamper occurs the red ‘Alert’ LED lights and the display shows:

```
IMK missing.

Recovery mode…
```

A unit which has had a positive tamper must be returned to AEP Networks to be recovered.

When an operational tamper occurs the red ‘Alert’ LED lights and the display is either:

```
Clear Status?

VEXT_OOS
```

- For a tamper caused by the external voltage being negative or too high.

```
Clear Status?

TEMP_DIFF
```

- For a tamper caused by the temperature changing too rapidly.

To recover from the tamper:

1. Press ENT

2. Insert the first SO smart card into the smart card reader when the following prompt appears. Enter the associated PIN and press ENT.

```
Insert Card SO 1

?
```

3. Repeat step 2 for the remaining SO cards required to authorize the Security Officer.

4. The Keyper will then return to the standard secured display:

```
Secured 9860-2    >

1.Set Online
```

During the tamper the SMK and Application Keys will have been destroyed. To fully recover the unit:

1. Re-import the backed up SMK (See Key Mgmt: SMK: Restore SMK)

2. Re-import the backed up Application Keys (See Key Mgmt: App Keys: Restore)

9 Audit Events

All security related operations (i.e. primarily local key management operations) are audited with the time and date of occurrence together with an event number, and for a number of audit event types, a relevant parameter. No security information is divulged by the audit log.

When the internally held audit log is full, new events begin to overwrite the oldest events. Under typical usage the audit log can contain many months of audits events. The audit log may be backed-up using the Keyper Management Centre. Please refer to Keyper Management Centre Manual (part number 011432).

All events can be viewed in real time by attaching a terminal to the serial port on the back of Keyper. For example, a Personal Computer running a terminal emulator connected via a USB to serial converter.

See the appendices for a full list of audited events.

10 Troubleshooting

If you encounter any problems using Keyper, AEP Networks recommends that you try the following:

Problem/Message	Possible cause	Suggested action
Power LED is not lit	There may be a problem with the mains supply or the PSU	
ALERT LED is lit	A tamper has occurred	Refer to the "Recovering from a Tamper" section
READY LED is flashing and the display says "Self Testing"	There is either a self-test in progress or Keyper has failed	Details of a failure will be output via the serial port
Invalid Card	This smart card is not the right type (i.e. AAK smart card instead of SMK) This smart card is not a part of a preloaded set (i.e. The first SMK smart card has been already loaded, the second one is a SMK smart card but not from the same set)	All operations requiring smart cards

Problem/Message	**Possible cause**	**Suggested action**
Invalid Card Set	After loading a full set of smart cards, recalculated information do not match smart card recorded information (corrupted smart card or incompatible version)	All operations requiring a set of smart cards
Card Error xxxx	The smart card driver has returned a smart card error	All operations requiring smart cards
Out Of Memory	Not enough memory to perform an operation: power down the Keyper and repeat the operation	All operations
Fatal Error XXXXX	See appendices	All operations
Invalid Time	A wrong number of seconds, minutes, and the year entered	Set clock menu
Access Denied	The operation is denied, the current Keyper state does not allow this operation	Application Key backup/import if services running Unsecured menu/import item (AAK already imported) SMK Import if services not running and Key Export enabled SMK menu/backup item (SMK already exported) Start Service if HSM is in Secured State & online, i.e. services already started

Problem/Message	Possible cause	Suggested action
Failed	Operation has failed	App Key menu /backup item App Key menu/import item (a key cannot be imported)
Corrupted Backup	Cannot decompress the buffer built from smart cards	App Key menu/import
Invalid PIN	An incorrect PIN has been entered	All smart card operations involving card with PIN (Security officer cards or Application Keys)
Old PIN=New PIN	The former PIN is the same as the new one	Security Officer menu/Change PIN item (Security officer cards or Application Keys)
Conf PIN=New PIN	The confirmation PIN has been entered incorrectly, it does not match the new PIN entered	Security Officer menu/Change PIN item (Security officer cards or Application Keys)

Stuck in 'Self-Testing'

To diagnose this, connect a computer running a terminal program such as miniterm, kermit or hyperterminal to the Keyper using a standard 9 pin computer to computer serial cable. Set up the serial port on the computer to 115,200 baud, no parity, one stop, one start, no flow control (i.e. no XON/XOFF, no RTS/CTS, no DTR, no CD and no DSR).

Power cycle the Keyper (power down and then up) and then capture the output. Send the output to AEP Networks Support.

Faulty Front Panel

Press the restart button. If the panel displays 'Self Testing' and the Keyper reports itself booting via the serial port (i.e. the normal start up sequence after reset or power up) the front panel may have a fault.

Network problems

If the LINK LED is not lit, check that the network cable is of the correct type. It should be a straight through cable if connecting to an MDI-X port, e.g. on a hub or switch. It should be a crossover type if connecting to an MDI port, e.g. a PC card.

Ensure that the network cable is connected correctly at the remote end. If necessary, disconnect the cable and then reconnect it securely.

Check that the remote end port is securely connected.

If the driver fails to contact Keyper carry out the following checks:

Check that a “ping” contacts the Keyper

The cryptographic services should have been started by a Security Officer

No two Keypers attached to the subnet should have the same IP address

The IP addresses or port numbers set up in the host machine or Keyper should have not changed unless the unit in which the change has been made has been rebooted

If a Keyper has been replaced by another with the same IP address the host machine should be rebooted

The Keyper outputs information via the serial port on which IP addresses are creating connections with it (when the connection is created) and where possible where the connection is closed.

Hardware Compatibility Problems

The Keyper supports 10Mb, 100Mb and 1Gb Ethernet networks.

The following are not guaranteed to be compatible with the Keyper:

- Third party network load balancing hardware
- IPSEC or TLS/SSL protected links between the Keyper and PKCS11 Provider Gateways
- MTU > 1,500

Appendix A. State name changes from Model 9720

Keyper Plus Model 9860 version 1	**Keyper Model 9720 and 9620**	**Meaning**
Unsecured	Initialised	Unit as shipped by AEP Networks The unit must be secured using a set of Security Officer cards
Secured and offline	Operational (Managed)	Unit after Security Officer cards have been issued and used to change state Unit cannot accept calls via PKCS11 / CAPI Providers
Secured and online	Operational	Unit after Operator cards have set the unit online Unit can accept calls via PKCS11 / CAPI Providers
Tampered	Tampered	Unit has been tampered, the SMK and Application keys have been positively erased
Download	Download	Unit is accepting a firmware download

Appendix B. Card role changes from Model 9720

The new role of Crypto Officer has been introduced by the Model 9860 to be responsible for Key Management.

Task	**Keyper *PLUS* Model 9860** **Authorised by**	**Keyper Model 9720 v2.0** **Authorised by**	**Keyper Model 9720 v1.8** **Authorised by**
Change state to Secured/Operational	m of n Security Officers	m of n Security Officers	2 of 2 Security Officers
Set online/offline (Start Services on Model 9720 v1.8)	m of n Operators	m of n Operators	1 Security Officer
HSM Management	m of n Security Officers	m of n Security Officers	2 of 2 Security Officers
Key Management	m of n Crypto Officers	m of n Security Officers	2 of 2 Security Officers
Clear tamper status	m of n Security Officers	m of n Security Officers	2 of 2 Security Officers

Appendix C. Menu structure changes from Model 9720

The Menu structure for Keyper ^{PLUS} Model 9860 is shown below together with how it differs from previous major releases. Where an entry is for example Operator:Dump Status it refers to the menu option 'Dump Status' as a sub menu option of the menu 'Operator'.

If a column is blank, that version of the Keyper did not support it.

Unsecured State: menu

Keyper Model 9720 version 2	**Keyper ^{PLUS} Model 9860**
Issue Cards	Issue SO Cards
Restore AAK	Restore AAK
Go Operational	Secure
SMK Algo	*N/A – (Requested when securing)*
Key Export	Key Export
Output Status	HSM Info:Output Info
View S/W Vers	HSM Info:S/W Version

Keyper Model 9720 v2 mapping onto Keyper ^{PLUS} Model 9860

Secured State: menu

Keyper Model 9720 version 2	**Keyper ^{PLUS} Model 9860**
Set Online	Set Online

Keyper Model 9720 version 2	Keyper ^{PLUS} Model 9860
Set Offline	Set Offline
Set FIPS Mode	Set FIPS Mode
HSM Mgmt	HSM Mgmt
Key Mgmt	Key Mgmt
View Card	View Cards
View Network	HSM Info: Network
Output Status	HSM Info: Output Info
View FIPS mode	HSM Info: FIPS mode
View S/W Vers	HSM Info: S/W version
Change PIN	Change PIN

HSM Management: menu

Keyper Model 9720 version 2	Keyper ^{PLUS} Model 9860
HSM Mgmt:Auto Online	HSM Mgmt:Auto Online
HSM Mgmt:Change Clock	HSM Mgmt:Change Clock
HSM Mgmt:Set Network	HSM Mgmt:Set Network
HSM Mgmt:Issue Cards	Role Mgmt:Issue Cards
HSM Mgmt:Clear Card	Role Mgmt:Clear Role Card
HSM Mgmt:View Cards	HSM Mgmt:View Cards

Keyper Model 9720 version 2	**Keyper ^{PLUS} Model 9860**
HSM Mgmt:Go Operational	*N/A - No longer used*.
HSM Mgmt:Go Initialise	HSM Mgmt:Unsecure

Key Management: menu

Keyper Model 9720 version 2	**Keyper** ***PLUS*** **Model 9860**
SMK	SMK
App Keys	App Keys
AAK	Role Mgmt: Backup AAK, Role Mgmt: Clear AAK Card
Output Key Sum	Key Summary
Output Key Det	Key Details
API Settings	API Settings
Alg Settings	Alg Settings

Key Management: SMK menu

Keyper Model 9720 version 2	**Keyper** ***PLUS*** **Model 9860**
Generate	Generate SMK
Backup	Backup SMK
Restore	Restore SMK
Clear Cards Generate and Backup do this automatically	Clear Cards Generate and Backup do this automatically
View Cards	View Cards

Key Management: Application Keys menu

Keyper Model 9720 version 2	**Keyper *PLUS* Model 9860**
Backup	Backup (covers smart cards and USB memory sticks)
Restore	Restore (covers smart cards and USB memory sticks)
Legacy Backup	Legacy Backup
Legacy Restore	Legacy Restore
Clear Cards	Clear Media (now also clears USB memory stick)
View Cards	Media Contents (covers smart cards and USB memory sticks)
Erase App.Keys	Erase App.Keys

Key Management: AAK menu

Keyper Model 9720 version 2	**Keyper *PLUS* Model 9860**
Backup	Role Mgmt: Backup AAK
Clear Cards Backup does this automatically	Role Mgmt: Clear AAK Card Backup does this automatically
View Cards	Role Mgmt: View Cards

Key Management: API Settings menu

Keyper Model 9720 version 2	**Keyper ^{PLUS} Model 9860**
Key Import	Key Import
Key Export	Key Export
Asym Key Gen Sym Key Gen Sym Key Der Signing Verifying MAC Gen MAC Ver Enc/Dec Asym Key Delete Sym Key Delete	Asym Key Gen Sym Key Gen Sym Key Der Signing Verifying MAC Gen MAC Ver Enc/Dec Asym Key Delete Sym Key Delete
Output Key Sum Output Key Det	

Key Management: Alg Settings menu

Keyper Model 9720 version 2	**Keyper ^{PLUS} Model 9860**
Suite B	Non Suite B On / Off
Non Suite B	*N/A – Single menu on 9860 (see above)*

Appendix D. Firmware version mappings

The table that follows shows the version numbers of the software loaded in the hardware as displayed by the **View software version numbers** menu option.

Keyper *PLUS* Model 9860

Component	Version
Product	2.1
BBL	010
ABL	011
App	021

Appendix E. Smart card and USB stick types supported

There are a limited number of smart card types that can be used for the Security Officers and key storage. All smart card types are supplied by Gemplus.

Smart Card Manufacturers and Models

All MPEMV smart cards (also known as MPCOS-EMV) are manufactured by GemAlto.

MPEMV 8000 R5 are supplied with the Keyper by AEP Networks.

Smart card use	Keyper family only, smart card and USB memory stick support
AAK component	MPEMV R3, R4, R5 any size
Keyper SMK component	MPEMV R3, R4, R5 any size
Security Officer	MPEMV R3, R4, R5 any size
Crypto Officer	MPEMV R3, R4, R5 any size
Operator	MPEMV R3, R4, R5 any size
Application Key Backup	MPEMV R4 128K (Model 9720 v1.6 or earlier) MPEMV R5 any size (Model 9720 v1.8 or later, Model 9860) USB (USB Memory Stick Support) memory stick (Model 9860)
Configuration	MPEMV R3, R4, R5 any size (Model 9720 v2 or later, Model 9860)

Viewing Smart Card Types after format

After a smart card has been issued for the first time, its type (and serial number) can be viewed using various menus. The table below lists the possible types and what they represent. Note that xxxxxxxxxxxxxxxx refers to the serial number of the smart card.

Smart card type	Displayed (Model 9720 v2 and 9860)	Displayed (Model 9620 and Model 9720 to v1.8)	Keyper versions that can read this format
AAK component	AAK v0 xxxxxxxxxxxxxxxx	Z0A	All
HSP4000 SMK component (legacy)	n.a.	Z0S	All
Keyper SMK component	SMK v0 xxxxxxxxxxxxxxxx	B0S	All
Security Officer	SO v1 xxxxxxxxxxxxxxxx	B0O	All
Operator	OP v1 xxxxxxxxxxxxxxxx	n.a.	Model 9720 v2 Model 9860
Crypto Officer	CO v1 xxxxxxxxxxxxxxxx	n.a.	Model 9860
Configuration information	Config Card v0 xxxxxxxxxxxxxxxx	n.a.	Model 9720 v2 Model 9860

Application Key Backup (v0)	App v0 xxxxxxxxxxxxxxxx	B0K	All Model 9620 All Model 9720
Application Key Backup (v1)	App v1 xxxxxxxxxxxxxxxx	B1K	Model 9620 v2.2 and later All Model 9720 Model 9860
Application Key Backup (v2)	App v2 xxxxxxxxxxxxxxxx	B2K	Model 9620 v2.3 and later All Model 9720 Model 9860
Application Key Backup (v3)	App v3 xxxxxxxxxxxxxxxx	B3K	Model 9720 v1.8 and later Model 9860

Application Key Backup (v3) was introduced to allow use of different size smart cards.

Smart Card PINS

When entered, PINS are not echoed to the display.

The default PIN is '11223344'.

Smart card type	**PIN required ?**	**Number of PIN retries before lock (Model 9720 v2, Model 9860)**	**Number of PIN retries before lock (Model 970 v1.8)**
AAK component	No		

HSP4000 SMK component (legacy)	No		
Keyper SMK component	No		
Security Officer	Yes	5	3
Operator	Yes	5	n.a.
Crypto Officer	Yes	5	n.a.
Configuration information	Yes	5	n.a.
Application Key Backup (v0)	No		
Application Key Backup (v1)	No		
Application Key Backup (v2)	No		
Application Key Backup (v3)	No		

The configuration information smart card contains:

- API Settings
- Algorithm Settings
- FIPS mode

USB Memory Stick Support

Memory sticks must be pre-formatted. Keyper does not provide facilities for formatting USB sticks.

Supported filesystems:

- FAT 16
- FAT 32

Common filesystems that are NOT supported (this is not an exhaustive list):

- NTFS (Microsoft)
- EXT (GNU Linux, *BSDs)
- Reiser (GNU Linux, *BSDs)

Note that FAT is supported currently by most systems.

USB Memory Stick Security

Keyper is not able to execute any files that reside on a USB stick.

Keyper also features full data/code separation so code in data areas cannot be executed.

Appendix F. New features in Keyper

Keyper ^{PLUS} Model 9860 1.0:

This is the first release.

For owners of AEP Networks Keyper Model 9720 v2 units, these are the differences in Keyper ^{PLUS} Model 9860:

- New ECDSA (256, 384 and 521 bit key sizes) key generation and signing services.
- New ECDH (256, 384 and 521 bit key sizes) key exchange services.
- DSA is not supported.
- A new Crypto Officer role has been introduced. The Crypto Officer now has full control over Key Management. The Security Officers now only have control over HSM Management.
- Crypto Officers each have smart cards issued in sets of 'm' of 'n' cards (2 of 2 to 9 of 9). Each requires a PIN.
- Application keys can now be backed up and restored on USB memory sticks as well as on smart cards.
- The Keyper ^{PLUS} Model 9860 can store up to 15,000 keys.

New information

Battery life

Statistics (performance, number of signings etc)

Serial number

Time and date

Keyper ^{PLUS} Model 9860 2.0:

- Support added for legacy algorithms:
    - DSA 1024
    - RSA algorithms 1024 – 4096 (v1.0 supported 2048 – 4096)

Keyper ^{PLUS} Model 9860 2.1:

- Support of SHA-2 HashMAC and SPKM.
- Defence against the Bleichenbacher attack.
- Support of IPv6

Appendix G. Audited events

The following audit events are logged. All audit events contain the time and date the event occurred and Keyper serial number. All numbers are displayed as hexadecimal values.

Parameters are usually the smart card serial number (where it says Serial number) or the first 6 characters of the key label (first six characters of the PKCS#11 CKA_LABEL or the RSA Full Provider/SChannel Provider key container name as appropriate).

Log Events

Description	*Audit No*	*Parameter*
Audit log has been created	000000	
Audit log has been read	000001	

System Events

Note that algorithm self-tests will fail on occasion due to the statistical nature of random number and prime number checking. Self-tests occur on newly generated key pairs.

Description	**Audit No**	**Parameter**
Keyper is in Unsecured State	100001	
Allow calls via API (i.e. Keyper has been set online)	100002	

Description	Audit No	Parameter
Disallow calls via API (i.e. Keyper has been set offline)	100003	
Keyper has detected an operational tamper	100004	
Keyper has detected a POST failure	100006	Error code
Keyper expecting and awaiting software update	100007	
Keyper power down or reset detected	100008	
POST error: SPI (hardware) failure	100009	
POST error: real time clock (hardware) failure	10000A	
POST error: EEPROM (hardware) failure	10000B	
POST error: SKS (hardware) failure	10000C	
POST error: I2C (hardware) failure	10000D	
POST error: Timer (hardware) failure	10000E	
POST error: keypad (hardware) failure	10000F	
POST error: FPGA (hardware) failure	100010	
POST error: MMI (hardware) failure	100011	

Description	Audit No	Parameter
Internal software failure detected on startup	100012	
Battery low (issued every 10 hours)	100013	
Entropy (hardware) failure	100014	
POST error: IFPGA (hardware) failure	100015	
POST error: 10K (hardware) failure	100016	
POST error: 1741 (hardware) failure	100017	
POST error: algorithm self test failure	100018	

Management Events (all Keypers)

Description	**Audit No**	**Parameter**
The smart card reader is off-line	200001	
An unidentified smart card detected on component restore	200002	Serial number
An unidentified smart card detected on component backup	200003	Serial number
Keyper SMK restore failed	200004	Serial number
Keyper SMK restored successfully	200005	Serial number
Keyper SMK backup failed	200006	Serial number
Keyper SMK backed up successfully	200007	Serial number
SMK restore failed from HSP4000 formatted smart card	200008	Serial number
SMK restored successfully from HSP4000 formatted smart card	200009	Serial number
SMK backup failed to HSP4000 formatted smart card	20000A	
SMK backup successfully to HSP4000 formatted smart card	20000B	
No longer used	20000C	

Description	Audit No	Parameter
No longer used	20000D	
AAK restored successfully	20000E	Serial number
AAK restore failed	20000F	Serial number
AAK backed up successfully (one log generated per card)	200010	Serial number
AAK backup failed	200011	Serial number
Application keys backup failed	200012	Serial number
Application keys backed up successfully	200013	Serial number
Application keys restore failed	200014	Serial number
Application keys restored successfully	200015	Serial number
Selected Application key restored to the Keyper successfully	200016	Key label
Specified Application key restore to Keyper failed	200017	Key label
Application keys restoration completed	200018	
Security Officer smart card issue succeeded	200019	Serial number
Security Officer smart card issue failed	20001A	

Description	Audit No	Parameter
An internal Keyper error occurred	20001B	
SMK generated successfully	20001C	
Re-wrapping a key with the newly promoted SMK failed	20001D	Key label
Re-wrapping a key with the newly activated SMK succeeded	20001E	Key label
All keys deleted, Keyper returned to Unsecured State	20001F	
All Application Keys deleted	200020	
No longer used	200021	
No longer used	200022	
Menu operation authorised by Security Officer successfully	200023	Serial number
Security Officer authorisation denied	200024	Serial number
An SMK component restored successfully (one log generated per card)	200025	Serial number
Real Time Clock set successfully	200026	
Allow Key Export via an API call or smart card	200027	
Disallow Key Export via an API call or smart card	200028	

Description	**Audit No**	**Parameter**
(Operational) Tamper acknowledged successfully	200029	
No longer used	20002A	
No longer used	20002B	
AAK smart card cleared successfully	20002C	Serial number
SMK smart card cleared successfully (one log generated per card)	20002D	Serial number
Application Key smart card cleared successfully (one log generated per card)	20002E	Serial number
Operator/Security Officer smart card cleared successfully	20002F	Serial number
No longer used	200030	
No longer used	200031	
No longer used	200032	
No longer used	200033	
No longer used	200034	
AAK component successfully restored (one log generated per card)	200035	Serial number

Description	Audit No	Parameter
No longer used	200036	
Network settings can no longer be changed	200037	
Allow key import via API call	200038	
Disallow Key import via API call	200039	
Allow key export via API call	20003A	
Disallow Key export via API call	20003B	
Allow asymmetric Key generation via API call (RSA/ECDSA)	20003C	
Disallow asymmetric Key generation via API call (RSA/ECDSA)	20003D	
Allow symmetric Key generation via API call (AES/TDES)	20003E	
Disallow symmetric Key generation via API call (AES/TDES)	20003F	
Allow key derivation via API call (AES/TDES)	200040	
Disallow key derivation via API call (AES/TDES)	200041	
Allow signing via API call (RSA/ECDSA)	200042	
Disallow signing via API call (RSA/ECDSA)	200043	

Description	Audit No	Parameter
Allow signature verification via API call (RSA/ECDSA)	200044	
Disallow signature verification via API call (RSA/ECDSA)	200045	
Allow MAC generation via API call (AES/TDES)	200046	
Disallow MAC generation via API call (AES/TDES)	200047	
Allow MAC verification via API call (AES/TDES)	200048	
Disallow MAC verification via API call (AES/TDES)	200049	
Allow encryption/decryption via API call (AES/TDES)	20004A	
Disallow encryption/decryption via API call (AES/TDES)	20004B	
Allow symmetric key deletion via API call (AES/TDES)	20004C	
Disallow symmetric key deletion via API call (AES/TDES)	20004D	
Enabling key export via API failed because all key exports disabled	20004E	
Key deleted via API call	20004F	
Keyper will remain online on reset/power up	200050	
Keyper will not remain online on reset/power up	200051	

Description	Audit No	Parameter
Number of Operator smart cards to set the Keyper online has been decided	200052	
Number of Operator smart cards to set the Keyper offline has been decided	200053	
Keyper set into FIPS mode	200054	
Keyper set into non FIPS mode	200055	
SMK to be generated and used as an AES key	200056	
SMK to be generated and used as a triple DES key	200057	
Allow asymmetric key deletion via API call (RSA/ECDSA)	200058	
Disallow asymmetric key deletion via API call (RSA/ECDSA)	200059	
Output Key Summary Enabled	20005A	
Output Key Summary	20005B	
Allow key details to be output	20005C	
Disallow key details from being output	20005D	
Allow Suite B algorithms to be used by API calls (AES/ECDSA/ECDH)	20005E	

Description	Audit No	Parameter
Disallow Suite B algorithms to be used by API calls (AES/ECDSA/ECDH)	20005F	
Allow Non-Suite B algorithms to be used by API calls (RSA/TDES)	200060	
Disallow Non-Suite B algorithms to be used by API calls (RSA/TDES)	200061	
New AAK generated in Unsecured State successfully	200062	
Operator smart cards issued successfully	200063	
Operator smart cards issue failed	200064	
Configuration smart card cleared	200065	
Configuration information backed up on smart card successfully	200066	
Configuration information backup on smart card failed	200067	
All Application keys deleted from the Keyper	200068	
Operator smart card authorisation succeeded	200069	
Operator smart card authorisation failed	20006A	
Crypto Officer smart card authorisation succeeded	20006B	

Description	Audit No	Parameter
Crypto Officer smart card authorisation failed	20006C	
Auditor smart card authorisation succeeded (version 2)	20006D	
Auditor smart card authorisation failed (version 2)	20006E	
Operator smart card cleared	20006F	
Crypto Officer smart card cleared	200070	
Auditor smart card cleared (version 2)	200071	
Attempt to import Application Keys wrapped in the wrong type of SMK	200072	
Successfully imported Application Keys from USB	200073	
Failed to import Application Keys from USB	200074	
Successfully exported Application Keys to USB	200075	
Failed to export Application Keys to USB	200076	
Crypto Officer cards successfully issued	200077	
Failed to issue Crypto Officer cards	200078	
Not currently used	200079	

Description	**Audit No**	**Parameter**
Not currently used	20007A	
Not currently used	20007B	
Not currently used	20007C	
Not currently used	20007D	
Not currently used	20007E	
Application keys deleted from USB	20007F	

Appendix H. Tamper codes

Tamper	**Tamper Type**	**Code (hex)**
External Voltage out of specification	Operational	2
N/A	Not currently used	4
Physical Breach	Positive	8
Internal Voltage out of specification	Positive	10
External Tamper	Positive	40
N/A	Not currently used	100
Maximum storage temperature reached	Positive	200
Minimum storage temperature reached	Positive	400
Temperature change too rapid	Operational	800

Appendix I. Smart card error codes

Application error codes

Error	Code
An operation failed because an invalid parameter was supplied.	1006
Hardware error. Call AEP Networks support	1500
Key invalid for the operation This can happen for example if a non-FIPS key operation is selected and services have been started in FIPS mode	1208
Fatal Error The AAK is corrupted, the store key cannot be used as a valid key This can happen if the Black Store has been corrupted without tamper detection or if Keyper code has been updated with an incompatible version (the stored AAK is not recognized as a valid key by the new software)	120A
Restored Application Keys not wrapped by loaded SMK Indicates that the SMK in Keyper is not the SMK that wrapped the Application Keys being restored	120D
Key not exportable	120F
Storage key is missing	1218

Error	**Code**
SMK in an inconsistent state Keyper probably tampered, action: return Keyper to AEP Networks	1219
FIPS mode mismatch	121A
Failed operation	1406
Invalid format This can happen if for example the wrong padding format is selected	1600
Invalid Mode This can happen if for example the incorrect mode is selected for an encipher operation	1601
Invalid serial number Serial number for the box has not been retrieved correctly.	1602
MAC verification failed	2000
Signature verification failed	2001
No RNG seed	2300
RNG seed too long	2301
RNG seed too short	2302
Invalid prime strength	2303

Error	Code
No data requested Requested RNG data length is zero	2304
Invalid RNG algorithm	2305
RNG value held in BBRAM has been reset unexpectedly	23FF
Algorithm self-test failed	2400
RSA or DSA algorithm test before use error	2401
Invalid number of components to generate This can happen when backing up SMK or AAK cards if the incorrect number of components is selected for n of m back up.	2500
Invalid Component Length If the algorithm data component length is incorrect	2501
All components loaded For example while doing m of n key back up.	2502
Load not complete For example if not enough components have been given to the m of n calculation	2503
Save not complete M of n save did not complete	2504
All Components retrieved	2505

Error	Code
If m of n component calculation is sent too many components	
Number of components not set for an m of n calculation	2507
Invalid PIN entered for an individual key	2600
PIN entry cancelled	2601
PIN entry task failed	2603
Time/date entered incorrectly	3002
Incorrect number of components	C003
Wrong format of smart card has been entered	C007
Tried to import SMK but either there was no spare slot or the smart card is not an SMK smart card	C00A

Key Management error codes

Error	Code
On import, application key smart card contains no keys	1000

Error	Code
On export, no application keys found to export to smart card	1002

These errors are displayed (in hexadecimal value) in the message "Card Error XXXX".

Comment	Value
Unknown error (a catch-all)	8001
Card reader command error	8002
Communications or protocol error	8003
Reader can't handle this type of card	8004
ISO command error	8005
Command length error	8006
Card not powered	8007
Card malfunction	8008
Card has been removed (during command)	8009
Card drawing too much power	800A
Time-out on port i/o	800B
Card reader closed	800C

General card error codes

Error	Code
Catch all for unexpected error	9001
Card write failure	9002
No memory/ID available	9003

File access/selection error codes

Error	Code
Invalid file ID	9004
Wrong type of file	9005
Invalid file or descriptor	9006
Invalid access specifier	9007

Data/value error codes

Error	Code
Bad or inconsistent data	9010
Bad data length or out of range	9011
Invalid key value	9012

Permission error codes

Error	Code
Not authorisation - requires PIN	9020
Requires ciphered access	9021

PIN error codes

Error	Code
Invalid PIN policy (length)	9022

Error	Code
Invalid PIN referenced	9023
Invalid PIN value	9024
PIN locked	9025
Illegal PIN length	9026
Illegal character in PIN entry	9027
Illegal PIN entry	9028
PIN not entered	9029
Old PIN and new PIN are the same	902A
New PIN not confirmed	902B

Secure messaging error codes

Error	Code
Bad secure messaging checksum	9030
No secure messaging checksum	9031

Error	**Code**
Secure messaging not set up	9032

Initialisation and set up error codes

Error	Code
Token is already initialised	9041
Token is already open	9042
Card format incompatible	9043

Crypto errors

Error	Code
UI task cannot start	C001
Incorrect number of components	C003
AA data is missing or cannot be read	C004
Busy state during key back up & restore.	C006
Invalid ICC – smart card already configured for a different type of key back up	C007
Invalid ICC smart card checksum	C008

Error	**Code**
The current SMK state does not allow this operation	C00A
Failed to start / stop services	C00B
Cannot create task mutex	C00D
Cancel key pressed	C00E
Front panel key switched	C00F
Unable to read firmware versions	C011
Date entered to locate key has invalid format	C019
No PIN defined for that key	C01A
Too many keys found with the search string criteria	C01B
Smart card is full – cannot add another key	C01C

Ultra
ELECTRONICS

www.ultra-aep.com