Advanced Configurable Cryptographic Environment (ACCE) v2

FIPS 140-2 Security Policy Iss 12

Table of Contents

1. Introduction

1.1. Scope

This document is the FIPS PUB 140-2 Security Policy for the AEP ACCE 2 v2.

It covers the following as used in the AEP Keyper Model 9720 Professional and the AEP Keyper Model 9720 Enterprise:

Hardware	2730-G2
Firmware	v2

Note: Triple DES and AES algorithms are carried out entirely and always in hardware using the SafeNet SafeXel 1741 chip. All other algorithms are always carried out in hardware.

1.2. Overview and Cryptographic Boundary

The *AEP ACCE 2 v2* (see front cover picture) is a *single user, multi-chip embedded* crypto-module. The FIPS PUB 140-2 cryptographic boundary is the metal case containing the entire AEP ACCE 2 v2.

Like its successful predecessors, the ACCE and ACCE-L3 modules, the AEP ACCE 2 v2 exists to provide cryptographic services to applications running on behalf of its user which communicate with it via a standard 10/100 Base T Ethernet interface using IP protocols. To implement these services, the module additionally requires a suitable power supply, Smart Card reader, digital display device, keypad and line drivers.

The AEP ACCE 2 v2 is usually sold embedded within a stand-alone “network appliance” Hardware Security Module [HSM] - type product such as the AEP Keyper Model 9720 (below).

The AEP Keyper HSM is typically used wherever secure storage and generation of cryptographic keys are required, especially where high performance cryptographic acceleration is desired.

1.3. Module Security Requirements

The module meets the overall requirements applicable to Level 4 Security for FIPS 140-2

Security Requirements Section	Level
Cryptographic Module Specification	4
Cryptographic Module Ports and Interfaces.	4
Roles, Services and Authentication	4
Finite State Model	4
Physical Security (Multiple-Chip Embedded)	4
Operational Environment	N/A
Cryptographic Key Management	4
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	4
Self-Tests	4
Design Assurance	4
Mitigation of Other Attacks	N/A[1]
Cryptographic Module Security Policy	4

[1] Although no specific resistance to other attacks is claimed (or has been tested), it should be noted that the module includes a number of active electronic devices and will typically be executing a number of processes in parallel in response to any requested cryptographic operation. This makes it difficult for an attacker to carry out timing or power analysis attacks as the “effective noise level” is high.

1.4. Module Ports & Interfaces

The module has dedicated, separate physical connections for power (dedicated connections), tamper[2], key backup and recovery (Smart Card), control interface (keypad & display), audit (serial port) and user data (Ethernet).

All connections to the module are via a 100-way ribbon cable. The following table describes the relationship between the physical connections available via this ribbon cable and their logical interfaces. (The module has no other electrical connections.)

Logical Interface	Data Type	Physical Interface
Data Input interface	User Data	Ethernet (shared with user logical Data Output Interface).
	Authentication Data	Smart Card.
	CO Data (Key Recovery)	Smart Card.
Data Output interface	User Data	Ethernet.
	Authentication Data (New User Creation)	Smart Card.
	CO Data (Key Backup)	Smart Card.
Control Input interface	CO & Operation functions	Front panel key pad.
	User Commands	Ethernet.
Status Output interface	-	LED, LCD, Serial.
Power Interface	-	Various 5V and similar inputs – dedicated power supply appropriately safety &EMC certified for destination country required (supplied as standard with the product).

Mapping Physical and Logical Interfaces

The User Data (Ethernet) connection can accept data (for an encrypt or sign operation) or output (for a decrypt operation) plaintext, encrypted keys (when enabled) and ciphertext data (output of a decrypt operation). Logical distinctions between plaintext, encrypted keys and ciphertext are made in the Application Programming Interface (API).

The key backup and recovery port (Smart Card) is also used to authenticate users and crypto officers. As these are separate processes (a crypto officer must authenticate *before* he can utilize key backup or recovery functions) they are logically distinct.

[2] Most tamper signals (e.g., temperature, physical penetration, etc.) are detected within the module – but the module provides external connections that can be used to externally *force* a tamper response. These are provided so that products incorporating the module can implement features such as “emergency erase all” pushbuttons, etc.

2. FIPS and non-FIPS Operation

The AEP ACCE 2 v2 supports “FIPS Mode” and “non-FIPS mode” operation.

When in FIPS mode, only FIPS approved cryptographic algorithm and key generation mechanisms are available. Non-FIPS mode is a functional superset of FIPS mode with additional cryptographic algorithms and non-FIPS approved key derivation mechanisms available.

Keys generated by non-FIPS derivations cannot be used when operating in FIPS mode.

The operator interface can be queried to confirm if the module is operating in FIPS or non-FIPS mode. In the AEP Keyper Model 9720, this is displayed on the LCD front panel display in response to an operator menu function.

2.1. Algorithms

Algorithms can be used in FIPS mode except where indicated. Keys cannot wrap stronger keys i.e. 128 bit AES keys cannot be used to wrap 192 bit AES keys.

Note: Triple DES and AES algorithms are carried out entirely and always in hardware using the SafeNet SafeXel 1741 chip. All other algorithms are always carried out in hardware.

The TDES-MAC referred to in the table is partially carried out in hardware (the TDES part) and partially in firmware (converting that into the MAC).

The certificates for AES and (non-TDES-MAC) TDES in the table below refer to the SafeNet SafeXel 1741 chip only.

Algorithm	Certificates	Key/modulus/exponent Sizes	Notes
DSA	#411	1024 bit modulus only.	FIPS certified PRIME; PQG(gen); KEYGEN(Y); SIG(gen); SIG(ver); MOD (ALL).
DSA		512 to 960 bit modulus inclusive (in 64 bit steps).	**Non FIPS mode only**[3] FIPS certified PRIME; PQG(gen); KEYGEN(Y); SIG(gen); SIG(ver); MOD (ALL)
RSA	#603	1024 to 4096 bit (in 32 bit steps) with and without CRT. Public exponents of 3, 17 and 65537.	PKCS#1, X9.31 (FIPS mode) ISO 9796, X.509 & Encryption (non FIPS mode).
RSA		512 to 992 (in 32 bit steps) with and without CRT. Public exponents of 3, 17 and 65537.	**Non FIPS mode only**[4] PKCS#1, X9.31 (FIPS mode) ISO 9796, X.509 & Encryption (non FIPS mode).
Diffie-Hellman		512 to 4096 bit modulus. Private key of between 160 bits and the modulus length (PKCS#3) (ephemeral/static not relevant).	**Non FIPS mode only**[5] X9.42 (ephemeral and static) not supported.
SHA-1	#1152	Bytes.	
SHA-2	#1152	224, 256, 384 and 512 bit in bytes.	
DES		ECB (e/d), CBC (e/d).	**Non FIPS mode only**[3] Encrypt/decrypt/MAC/verify.
TDES	#210	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2).	Hardware implementation
TDES	#896	TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2).	Firmware implementation
TDES-MAC	#896		(Vendor Affirmed).
AES	#96	128, 192, 256 bit. ECB CBC.	Hardware implementation
AES	#1257	128, 192, 256 bit. ECB CBC.	Firmware implementation
RNG	#699	FIPS 186-2 Appendix 3.1 based RNG continually re-seeded by hardware Random Noise Source.	
MD-5		Bytes.	**Non FIPS mode only**[3]

2.2. Key Generation

The module features a FIPS-approved random number generator (RNG) based on SHA-1. This RNG is used to produce random numeric values for cryptographic keys, for random vectors where required by a padding technique and in response to the API utility function “randomgenerate”. All user keys generated by the module rely on this RNG, thus all user keys *generated while in “FIPS mode”* are “FIPS keys”.

[3] Attempts to access non-FIPS operations while in FIPS-mode fail and error code 0x1400 (K_MECHANISM_NOT_AVAILABLE) is returned.
[4] Attempts to access non-FIPS operations while in FIPS-mode fail and error code 0x1400 (K_MECHANISM_NOT_AVAILABLE) is returned.
[5] Attempts to access non-FIPS operations while in FIPS-mode fail and error code 0x1400 (K_MECHANISM_NOT_AVAILABLE) is returned.

2.2.1. Key Generation Detail

The RNG is itself seeded by a built in electronic circuit which utilizes a random noise source. This circuit develops 32 bits of "hardware entropy" every 64 milliseconds – and this is used to reseed the RNG at that frequency.

Symmetric keys are generated by utilizing the output of the RNG and setting appropriate padding where required by the intended algorithm.

Finally, all Asymmetric key pairs generated are subject to a pairwise consistency test (a trial "sign/verify").

2.2.2. Random Number Continual Self Tests

Both the RNG and the hardware source entropy source used to continually seed it are continually tested as specified by FIPS PUB 140-2 section 4.9.2 paragraph 1. If a failure occurs, the AEP ACCE 2 v2 will report an error whenever a "get random" or "key generation" operation is made and the operation will fail.

2.2.3. Non FIPS-mode Key Generation

Non FIPS mode also support commercial Key derivation mechanisms. Keys derived via these mechanisms are *not* "FIPS keys" and are not available when operating in FIPS mode.

3. Tests

Three types of tests are carried out:

Self Tests: these are carried out on power up/reset

Continual Tests: these are carried out when appropriate and on a continual basis

Firmware Load Test: the test that takes place when the firmware update is downloaded

3.1. Self Tests

At power up and at reset (reset – and hence self testing - can be demanded by operator action), all hardware and firmware components necessary for correct operation are self-tested.

This self testing is carried out on the principle of "test before use" and hence the test ordering is:

1. Components necessary for minimal self-test environment:

   CPU cache.
   CPU register set.
   CPU time base ("decrementer")
   Read/Write memory.

2. Components necessary for full self testing:

   Read Only Memory.
   Internal interface devices.
   Secure Key Store.
   Cryptographic accelerator circuit test.

3. Application firmware:

   Integrity check (utilizing TDES MAC function).

4. Cryptographic Algorithms:

- RNG known answer test
- AES known answer test
- TDES known answer test
- 1024 bit DSA known answer test
- 1024 bit RSA known answer test
- SHA-1 known answer test

- SHA-224 known answer test
- SHA-256 known answer test
- SHA-384 known answer test
- SHA-512 known answer test

Any failure will cause the module to halt and display an error status message via the serial port. If the failure occurs in any of the components identified in '1. Components necessary for minimal self-test environment:' it is possible that no message will be output as the fault may be so severe as to prevent this operating.

All cryptographic operations (including user and crypto officer log in) are inhibited if any self tests fail.

3.2. Continual Tests

The following are tested continually:

- Random Noise source test, test for (non) consistency
- RNG conditional self test
- DSA pair wise consistency test
- RSA pair wise consistency test

3.3. Firmware Load Test

The module can accept field updates to its internal firmware. These updates are digitally signed using the RSA algorithm and verified by a public key which is built into the module during factory commissioning.

The loading of any firmware that is not FIPS 140-2 validated renders the unit a non-FIPS validate unit.

4. Physical Security

4.1. Introduction

The AEP ACCE 2 v2 is an embedded module validated as meeting the requirements of FIPS PUB 140-2 level 4.

Essentially this means that any physical attempt to access the module's Critical Security Parameters (CSPs) will result in those parameters being actively erased (zeroized).

This protection is achieved by the construction of the module. All electronic elements are surrounded by a tamper-detecting envelope within an opaque resin coating and an outer metal case. Attempts to physically access the cryptographic processor and/or associated devices (including cutting, chemically dissolving, heating, cooling or modulating power supplies) cause the module to halt and to zeroize all CSPs.

4.2. Physical Security Rules

The AEP ACCE 2 v2 will detect and respond to (by zeroizing keys) all types of physical, electrical and environmental attacks that are envisaged by the FIPS 140-2 standard. No operator inspections, etc. are required for *secure* operation; the module will stop operating in the event of a tamper event.

(It is important, however, to regard any and all instances of unexpected "tamper events" as serious and possibly an indication of an attack.)

For *reliable* operation it is necessary that the permanent power supply to the module is maintained. Removal of this power supply will cause a "positive tamper" event and the module will need to be returned to AEP for repair. In the AEP Keyper Model 9720, this permanent power supply is provided by an internal battery – the AEP ACCE 2 v2 warns if the supply voltage drops significantly and this is an indication that that battery should be replaced.

5. Identity Based Authentication

5.1. Single User

The AEP ACCE 2 v2 supports multiple users - but only one may have an active session at any time.

5.2. User/Crypto Officer Authentication

The AEP ACCE 2 v2 user authentication mechanism uses a Gemplus MPCOS compatible Smart Card reader/writer connected to the appropriate interface.

A User requires between 2 and 9 *Matched* Smart Cards (m from a set of n) in order to identify and authenticate themself. A Crypto Officer requires between 2 and 9 *Matched* Smart Cards (m from a set of n) in order to authenticate themself. User and Crypto Officer cards are separate and not interchangeable between roles.

(The requirement for a Matched set of Smart Cards allows customers to operate a "4+ eyes" policy where at least two people are required to work together (with one Smart Card of a set each) in order to access User/Crypto Officer Functions.)

5.3. Creating a User or Crypto Officer

The AEP ACCE 2 v2 directly supports "user creation". Once operational a set of Crypto Officers are required to create sets of "users" or further sets of "crypto officers".

The procedure creates matched sets of cards that contain a unique ID number (the ID is unique to each *card*) and a unique 56 bit cryptographic secret. Later authentication of this new Crypto Officer requires *at least two* cards in this set.

5.4. Strength of Authentication Mechanism

In order to authenticate, a User must possess the appropriate 56 bit secret "key". This key is used to encrypt a random DES challenge - the probability of a correct response to the random challenge is directly related to the key space - i.e. $1:2^{56}$.

Using the supplied interface, a "brute force" attack on this key could be attempted once every 5 seconds – but a sufficiently skilled attacker *could* develop equipment capable of conforming to the front panel interface definition and therefore simulating operation of the front panel keys in response to prompts and replies to the random challenge more rapidly than a human operator could achieve.

In that situation, the rate that challenges can be issued is limited by the sum of the time to generate a random challenge, the time to encrypt a response, the time to decrypt the response and the time to pass this data together with front panel menu data over a 9600 baud serial link.

As the entire protocol involves at least 100 bytes of data, the attacker is limited to a maximum of 10 attacks per second by the line speed.

Accordingly, the average time taken to discover the key is *at least*:

$2^{56}/2 * 0.1$ seconds. ($3.6 * 10^{15}$ seconds; $6 * 10^{13}$ minutes; slightly more than 115 *million years*)

FIPS PUB 140-2 requires a probability of less than 1 in 100,000 of false acceptance within one minute. As illustrated, the module significantly exceeds this.

6. Roles and Services

6.1. Roles

The AEP ACCE 2 v2 supports the following Roles:

Role	Authentication Type	Authentication Data
Operator	None	None[6].
User	Identity-based (Unique ID Number)	Knowledge of a set of individual DES keys – the module generates "m" random numbers (one per card) and requires the result of a DES ECB encryption of that number using that key for each card.
Crypto-Officer	Identity-based (Unique ID Number)	Knowledge of a set of individual DES keys – the module generates "m" random numbers (one per card) and requires the result of a DES ECB encryption of that number using that key for each card.

6.1.1. Operator

In addition to the authenticated roles of User and Crypto Officer mentioned in "5. Identity Based Authentication", the module supports a non-authenticated "operator" role. The operator role only permits the modules IP address, net mask and port numbers to be viewed, a card's type and serial number, the device's FIPS mode and the firmware version numbers to be inspected, the device's non-critical security parameter configuration to be output to the serial port and a hard reset to be initiated. The operator role cannot undertake any cryptographic operations or load or unload keys, etc. The operator role has no access to CSPs.

6.1.2. User

All cryptographic functions (in both FIPS and non-FIPS modes) provided by the module require that an *Authenticated User* is "logged in".

When a User logs in, they carry out a "Set Online". This enables the network API and all enabled cryptographic functions and all user keys are available until the user either carries out a "Set Offline" ("logs out") or (if configured) the operator executes a reset (or cycles the module power).

"FIPS mode" or "Non-FIPS mode" can be selected "crypto officers" from the device's menu. "Non-FIPS mode" is a functional superset of FIPS mode and enables non-FIPS approved cryptographic algorithms and key derivations.

Once set on-line, users can carry out all cryptographic functions, import and export *protected*[7] keys (where enabled) over the network interface, generate keys (specifying if future export over the network interface is permitted) and random numbers, etc.

[6] The module does not authenticate the operator role at all; a switch closure on an interface line to activate the operator interface. In the AEP Keyper Model 9720, this interface line is wired to a keyswitch.

[7] i.e. encrypted keys

Users have no access to *module* CSPs. Users cannot access or modify the Storage or Image master keys, cannot access the Smart Card interface to backup or recover keys, etc. Users cannot create other User or Crypto Officer Smart Card sets.

6.1.3. Crypto Officer

A Crypto Officer cannot act as a *User* . However Crypto Officers can access the Smart Card interface in order to perform master key backup[8] or recovery and user key backup and recovery.

The Crypto Officer can also disable all protected key import and export over the network interface, can create additional user and crypto officer Smart Card sets and erase all keys. "Go Initialised" sets the module to "Initialized State" and revokes all User and Crypto Officer Smart Card sets.

Once in initialized state, the module cannot be used until it is made operational again (by generating an initial set of Crypto Officer Smart Cards and deliberately "going operational") and being set on-line (by generating an initial set of User Smart Cards and deliberately selecting "Set Online").

6.2. Services and Critical Security Parameter (CSP) Access

6.2.1. CSP Definition

The following table describes the keys and CSP's stored or used by the module or used to sign firmware downloaded into the module:

CSP Name	Description and /or Purpose	Type of Key or CSP	Storage Location
IMK (Image Master Key)	Protection of the SVK, SSMK & AAK	Triple DES	SKS[9]
ISMK (Internal Storage Master Key)	Protection of User Keys stored internally in BBRAM	256 bit AES	SKS[9]
SMK (Storage Master Key)	Protection of User Keys backed up to smart cards	192 bit Triple DES or 256 bit AES	SKS[9]
AAK (Authentication String)	Authentication of Users & Crypto Officers	128 bit secret random value.	BBRAM, TDES encrypted by IMK.
User Keys	Encryption/Decryption, or Signatures	Triple DES, AES, DSA, RSA	BBRAM, TDES encrypted by SMK.
SSMK (Software Storage MAC key)	Validation of firmware at power up or reset.	Triple DES	BBRAM, TDES encrypted by IMK.
SVK (Software Verification Key)	Verify Firmware Downloaded to Module	4096 bit RSA public key	BBRAM, TDES encrypted by IMK.
CSVK (Software Verification Key)	Verify Firmware Downloaded to Module	4096 bit RSA public key	BBRAM, TDES encrypted by IMK.
SEK (Software Encryption Key)	Decryption of firmware update downloaded to Module; downloaded as a part of the firmware update 'blob'.	192 bit Triple DES	Transient session key; not stored; erased after firmware decrypted.
SKEK (Software Key	Decryption of Software	192 bit Triple DES	BBRAM, TDES

[8] key backup is not possible if it has been disabled during initialisation of the module – this is to support the digital signature laws of various European states.

[9] The Secure Key Store (SKS) is a dedicated micro controller with its own internal memory that permanently monitors the tamper status of the module and zeroizes its contents (the SMK & IMK) if a tamper occurs. It contains the IMK, ISMK and SMK in plaintext.

Encryption Key)	Encryption Key (SEK).		encrypted by IMK.
TDES MAC	Verify firmware integrity at power-on	DES MAC result	Stored in FLASH at end of firmware image.
RNG Seed	RNG Seed	160 bits	Dynamic RAM

6.2.2. Services and Access

The table below summarizes the CSPs accessed by the various roles in utilizing the module's services. (Note all Operator services are available to Users. All Operator but no User Services are available to Crypto Officers.). All services are carried out in FIPS mode unless otherwise stated.

Role	**Services**	**Notes**	**Access (RWX)**
Operator	View Network Parameters	-	R
Operator	View Firmware Version	-	R
Operator	View FIPS Mode	-	R
Operator	View card type	-	R
Operator	Execute Self Tests	-	X
Operator	View Audit Log	-	R
Operator	View HSM Status (Output Status)	-	R
User	Authenticate	An authentication secret is derived from the AAK and the User ID values. User responds to a random challenge by DES encrypting it with his copy of this secret and returning the result.	AAK - X
User	Change PIN	Change User smart card PIN.	W
User	Generate Key	RSA, DSA, TDES, AES.	User Key - W
User	Sign	RSA, DSA.	User Key - X
User	Verify	RSA, DSA.	User Key - X
User	Encrypt/Decrypt	TDES, AES.	User Key - X
User	Key (un)wrap	TDES, AES, RSA.	User Key - X
User	Hash data	SHA-1, SHA-2.	X
User	Get Random	RNG.	X
User	Non FIPS mode:	< 1024 bit RSA, < 1024 bit DSA.	User Key - X

Role	Services	Notes	Access (RWX)
	Sign		
User	Non FIPS mode: Verify	< 1024 bit RSA, < 1024 bit DSA.	User Key - X
User	Non FIPS mode: Encrypt/Decrypt	56 bit DES.	User Key - X
User	Non FIPS mode: MAC	DES, TDES, AES.	User Key - X
User	Non FIPS mode: MAC Verify	DES, TDES, AES.	User Key - X
User	Non FIPS mode: Key Exchange	Diffie Hellman	User Key - X
User	Non FIPS mode: Derive Key	DES, TDES	User Key – W, X
Crypto Officer	Set module operational	AAK.	AAK - X
Crypto Officer	Authenticate	An authentication secret is derived from the AAK and the User ID values. User responds to a random challenge by DES encrypting it with his copy of this secret and returning the result.	AAK - X
Crypto Officer	Change PIN	Change Crypto Officer smart card PIN.	W
Crypto Officer	Modify Network Parameters	Although the Crypto Officer can modify network parameters they do not become effective until the next restart of the module and an authenticated user has logged in.	W
Crypto Officer	Permanently disable all key export	Must be set before making module operational. (Also disables SMK backup/recovery.)	X
Crypto Officer	View key names and HSM status	Outputs the number of keys stored by type, algorithm and key length out of the serial port.	R
Crypto Officer	Create New User	Creates new smart card sets (M of N) containing new authentication secrets on 2 of 4 to 9 of 9 Smart Cards.	AAK - X

Role	Services	Notes	Access (RWX)
Crypto Officer	Generate SMK		SMK - W
Crypto Officer	Backup SMK	SMK (M of N components; La Grange interpolating Polynomial, one component per Smart Card, 2 of 4 to 9 of 9). SMK backup can be disabled during initialization in order to confirm to the Digital Signature laws of some European states.	SMK - R
Crypto Officer	Recover SMK	SMK (M of N components; La Grange interpolating Polynomial, one component per Smart Card, 2 of 4 to 9 of 9). SMK recovery can be disabled during initialization in order to confirm to the Digital Signature laws of some European states.	SMK - W
Crypto Officer	Export AAK	AAK (N of N components; XOR, one component per Smart Card, 2 of 2 to 9 of 9).	AAK - R
Crypto Officer	Backup User Keys	User keys are copied to the module internal non-volatile store from smart cards. When backed up they are decrypted with the ISMK and re-encrypted with the SMK before storage in the smart card's internal non-volatile store. User Key backup can be disabled during initialization in order to confirm to the Digital Signature laws of some European states,	User Keys – W SMK – X ISMK - X
Crypto Officer	Recover User Keys	User keys are copied to the module's internal non-volatile store from smart cards. When recovered they are decrypted with the SMK and re-encrypted with the ISMK before storage in the modules internal non-volatile store. User Key recovery can be disabled during initialization in order to confirm to the Digital Signature laws of some European states,	User Keys – W SMK – X ISMK - X
Crypto Officer	Zeroize All Keys	Zeroize ALL CSPs (except IMK, SSMK, SVK, CSVK or SKEK). Revokes all User and Crypto Officer Smart Cards. Returns module to “as delivered” state.	SMK, AAK & User Keys – X. (All zeroized)
Crypto Officer	Delete All User Keys	Delete All User Keys (not including SMKs, AAK, IMK, SSMK, SVK, CSVK, or SKEK).	User Keys – W (All zeroized)

Role	Services	Notes	Access (RWX)
Crypto Officer	Set FIPS/Non-FIPS Mode	Sets the HSM into FIPS/Non-FIPS mode.	User Keys – X
Crypto Officer	Enable or disable key import via API	Allows/disallows key import (wrap) via the API.	User Keys – W
Crypto Officer	Enable or disable key export via API	Allows/disallows key export (unwrap) via the API.	User Keys – R
Crypto Officer	Enable or disable Asym key pair generation for use with API	Allows/disallows DSA/RSA key pair generation via the API.	User Keys – W
Crypto Officer	Enable or disable Sym key generation for use with API	Allows/disallows AES/triple DES key generation via the API.	User Keys – W
Crypto Officer	Enable or disable signature generation for use with API	Allows/disallows DSA/RSA signing via the API.	User Keys – X
Crypto Officer	Enable or disable verification for use with API	Allows/disallows DSA/RSA signature verification via the API.	User Keys – X
Crypto Officer	Enable or disable encryption /decryption for use with API	Allows/disallows AES/triple DES encryption or decryption via the API.	User Keys – X
Crypto Officer	Enable or disable Asym key deletion for use with API	Allows/disallows DSA/RSA keys to be deleted via the API.	User Keys – W (All zeroized)
Crypto Officer	Enable or disable Sym key deletion for use with API	Allows/disallows AES/triple DES keys to be deleted via the API.	User Keys – W (All zeroized)
Crypto Officer	Enable or disable Suite A and/or Suite B functions for use with API	Allows/disallows Suite A and/or Suite B algorithms to be used via the API. A 'disable' overrides all enables elsewhere (e.g. AES encryption/decryption in not allowed if Suite B is disabled, DSA/RSA signing is not allowed if Suite A is disabled. An 'enable' does not override other disables elsewhere.	User Keys – RWX

Role	Services	Notes	Access (RWX)
Crypto Officer	Backup settings	The above enable/disable settings can be saved to smart card.	RW
Crypto Officer	Recover settings	The above enable/disable settings can be restored from smart card.	RW
Crypto Officer	Output key summary	Outputs the number of user keys stored in the module (by algorithm/key size) to the serial port.	R
Crypto Officer	Output key details	Outputs the algorithm/key size/name (not id)/key policy for each user key stored to the serial port.	R
User	Update firmware	Update the firmware: the firmware downloads' signatures (x2) are verified and the firmware decrypted. If the firmware is older than the current firmware the download is rejected.	WX

7. Maintenance

The AEP ACCE 2 v2 has no concept of a Maintenance role.

If a fault develops (including faults indicated by the self-test system), the module must be removed from service.

Repair of an AEP ACCE 2 v2 requires return to AEP Networks; no third party or site service is possible.

Please note, AEP is not aware of *any* mechanism which can recover customer's keys from an AEP ACCE 2 v2 without either access to the Security Officer authentication Smart Cards or key backup Smart Cards. AEP is not able to assist customers in key recovery if such backups are not maintained.

Appendix A Operator Guidance

Introduction

This section presents brief details of the installation, configuration and operation of a product based on the module including ensuring it is operated *in FIPS mode* should only be undertaken by suitably qualified and authorized personnel and in accordance with the instructions contained in the relevant product manuals.

However, the main points that must be observed in order to operate this module *in FIPS mode* are:

Inspection on Delivery

All products based on the module are delivered in tamper evident packaging – only authorized personnel should remove the product from its packaging and they should satisfy themselves that the packaging has not been tampered with before doing so. If the packaging shows evidence of tampering, this must be regarded as suspicious.

Initialization

Creating the First Crypto Officer

On delivery the module should be in "Initialized State" – at this point it has no security data in it at all and the first thing that must be done is the creation of the first Security Officer [SO].

On initial switch on the module will carry out self tests and then display "Important Read Manual" on the *product* LCD display panel. Upon selecting 'ENT' the user is prompted to Issue Cards (the first menu option):

"Initial 1126 >"
"1. Issue Cards."

or

"Initial 0405 >"
"1. Issue Cards."

At this point, press 1 on the product keypad, select the number of cards to be issued (N) and then the number of those issued cards to be used (M). When prompted insert each Smart Card of the set in turn[10]. For each card the Card's actual PIN must be entered when prompted for, the default for a new card is 11223344). (You can change this Card PIN later.)

When all cards have been initialized, the creation of the Crypto Officer card set is complete and you should proceed to "Go Operational" in order to complete the configuration and create any desired additional Crypto Officers and the first Users.

[10] Cards used to identify *Users* and *Crypto Officers* are termed "Operator cards" and "Security Officer Cards" respectively in product documentation.

"Going Operational"

Now the first Crypto Officer exists, the module should be made operational by selection menu item "3.Go Operational". The Crypto Officer will have to authenticate this command by inserting a subset (M) of the (N) SO cards and keying in their PINs as prompted.

Once the Crypto Officer has been authenticated the Keyper will prompt for a configuration to be imported. This options allows basic configuration details to be imported from smart card.

The next items to be prompted for are the Keyper's IP address, port number, net mask and the time and date (to set up the real time clock).

Finally the restart button should be pressed to ensure that the Keyper uses the new network settings.

When Operational the Crypto Officer should change their PIN using the 'Change PIN' menu option.

Operational State

Creating the First User

Select the "4.HSM Mgmt" menu option. The Crypto Officer will have to authenticate this command by inserting a subset (M) of the (N) SO cards and keying in their PINs as prompted. Once the Crypto Officer has been authenticated select the menu option "6.Issue Cards". At this point, Select the number of cards to be issued (N) and then the number of those issued cards to be used (M). When prompted insert each Smart Card of the set in turn[11]. For each card the Card's actual PIN must be entered when prompted for, the default for a new card is 11223344). (You can change this Card PIN later.)

When all cards have been initialized, the creation of the User (i.e. Operator smart card set) is complete.

Set on-line in FIPS mode

FIPS mode is the default.

From the front panel menu select "1.Set Online". The User will have to authenticate this command by inserting a subset (M) of the (N) Operator cards and keying in their PINs as prompted.

The READY LED will then turn on to indicate that the Keyper is on-line.

Confirm FIPS mode operation

From the front panel menu select "9.View FIPS mode" and ENT. The front panel display will now confirm the module is operating in FIPS mode by displaying "FIPS mode".

[11] Cards used to identify *Users* and *Crypto Officers* are termed "Operator cards" and "Security Officer Cards" respectively in product documentation.

Document Configuration

Document details

File Name:	**SecurityPolicy.doc**
Document Title:	**FIPS 140-2 Security Policy Iss 12**
Document Revision No.:	**Iss 12**
Author:	**David Miller – updated by Rod Saunders/David Miller**
Approved By:	**David Miller**
Revision Date:	**12th May 2010**