AEP Enterprise CM

(Version HW:2731_G1 issue 3 FW: 1.3)

011126 FIPS 140-2 Security Policy

Table of Contents

1. Introduction

1.1. Scope

This document is the FIPS PUB 140-2 Security Policy for the AEP Enterprise CM.

1.2. Overview and Cryptographic Boundary

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

Like its successful predecessors, the ACCE and ACCE-L3 modules, the AEP Enterprise CM 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, SmartCard reader, digital display device, keypad and line drivers.

The AEP Enterprise CM is usually sold embedded within a stand-alone "network appliance" Hardware Security Module [HSM] - type product such as the AEP Keyper Enterprise (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 (SmartCard), 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 (SmartCard) 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 Enterprise CM 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 Enterprise, 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.

Algorithm	Certificates	Key/modulus/exponent Sizes	Notes
DSA	#123	512 to 1024 bit modulus inclusive (in 64 bit steps).	FIPS certified PRIME; PQG(gen); KEYGEN(Y); SIG(gen); SIG(ver); MOD (ALL)
RSA	#32	1024 to 4096 bit (in 32 bit steps) with and without CRT. Public exponents of 3, 17 and 65537.	PKCS#1 (FIPS mode) ISO 9796, X.509 & Encryption (non FIPS mode)
Diffie-Hellman (Key Agreement)		512 to 4096 bit modulus. Private key of between 160 bits and the modulus length (PKCS#3) (ephemeral/static not relevant).	X9.42 (ephemeral and static) not supported.
SHA-1	#275	Bytes	
DES	#281	ECB (e/d), CBC (e/d), MAC.	For US Federal Systems, DES may only be used for legacy systems.
TDES	#290	TECB(e/d; KO 1,2,3); TCBC(e/d; KO 1,2,3	
TDES-MAC	#290		Vendor Affirmed
AES	#196	128 bit. ECB CBC	
PRNG	#41	FIPS 186-2 Appendix 3.1 based PRNG continually reseeded by hardware Random Noise Source.	
MD-5		Bytes	**Non FIPS mode only**[3]
XOR_BASE_AND_DATA		Derive DES or 3DES key from supplied key and supplied mask.	**Non FIPS mode only. (Note. Derived keys cannot**[4] **be accessed in FIPS mode.)**

[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 use derived keys while in FIPS-mode fail and error code 0x1208 (K_KEY_INVALID_FOR_OPERATION) is returned.

2.2. Key Generation

The module features a FIPS-approved (certificate #41) pseudo random number generator (PRNG) based on SHA-1. This PRNG 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 PRNG, thus all user keys *generated while in "FIPS mode"* are "FIPS keys".

2.2.1. Key Generation Detail

The PRNG 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 PRNG at that frequency.

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

Prime numbers generated as follows:

Generate random data of n bits.
Set the MSB and LSB to 1.
For RSA the 2nd most significant bit is also set so that the modulus pq is of the right size.
Confirm that the result cannot be divided by all prime numbers less than 256.

1. Perform Miller Rabin with the number of iterations of Miller Rabin per ANSI X9.31-1998, appendix B-2, to give a residual composite probability <2^-100:

<150 bits, 27 iterations
<200 bits, 19 iterations
<300 bits, 13 iterations
<400 bits, 10 iterations
<500 bits, 8 iterations
<600 bits, 5 iterations
>=600 bits, 4 iterations

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

2.2.2. Random Number Continuous Self Tests

Both the PRNG 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 Enterprise CM 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

When operating in non-FIPS mode, keys *generated* are generated using the same FIPS-approved PRNG as in FIPS mode. *Generated* keys are therefore "FIPS keys" and can be used in both FIPS and non-FIPS modes.

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.

2.3. 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.
   SafeNet 1741 circuit test.

3. Application firmware:

   Integrity check (utilizing TDES MAC function).

4. Cryptographic Algorithms:

   AES, DES, TDES, DSA known answer tests.
   Algorithms implemented in firmware (SHA-1, PRNG) known answer test.
   AEP 10K (RSA) known answer tests.

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 section 1, 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.

2.3.1. 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.

3. Physical Security

3.1. Introduction

The AEP Enterprise CM 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.

3.2. Physical Security Rules

The AEP Enterprise CM will detect and respond to (by erasing 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 Enterprise, this permanent power supply is provided by an internal battery – the AEP Enterprise CM warns if the supply voltage drops significantly and this is an indication that that battery should be replaced.

4. Identity Based Authentication

4.1. Single User

The AEP Enterprise CM supports multiple users - but only one may have an active session at any time.

4.2. User/Crypto Officer Authentication

The AEP Enterprise CM user authentication mechanism uses a Gemplus MPCOS compatible SmartCard reader/writer connected to the appropriate interface.

A User requires *One* SmartCard in order to identify and authenticate him (her) self. A Crypto Officer requires a *Matched Pair* of Smartcards in order to authenticate him (her) self.

(The requirement for a Matched Pair of Smartcards allows customers to operate a "4 eyes" policy where two people are required to work together (with one SmartCard of a set each) in order to access Crypto Officer Functions.)

4.3. Creating a User or Crypto Officer

The AEP Enterprise CM does not directly support "user creation"; it always creates Crypto Officers. The distinction between "users" and "crypto officers" is a procedural matter for customers as described below:

The procedure creates a matched pair 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 *both* cards in this pair. However, *either* card *on its own* can be used to authenticate for the User Role.

Thus to convert a Crypto Officer Card Set into a User Card, the customer simply destroys one of the matched pair of new Crypto Officer Cards. That card can then be used to activate a user session but – as its fraternal twin no longer exists – can never be used to activate Crypto Officer functions.

4.4. 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.

5. Roles and Services

5.1. Roles

The AEP Enterprise CM supports the following Roles:

Role	Authentication Type	Authentication Data
Operator	None	None[5].
User	Identity-based (Unique ID Number)	Knowledge of an individual DES key – the module generates a random number and requires the result of a DES ECB encryption of that number using that key.
Crypto-Officer	Identity-based (Unique ID Number)	Knowledge of a pair of DES keys – the module generates two random numbers and requires the result of two individual DES ECB encryptions of those numbers – one for each key.

5.1.1. Operator

In addition to the authenticated roles of User and Crypto Officer mentioned in "4, Identity Based Authentication", the module supports a non-authenticated "operator" role. The operator role only permits the modules IP address and port numbers to be viewed or altered, the firmware version numbers to be inspected 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.

5.1.2. 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, (s)he "starts services". This enables the network API and all cryptographic functions and all user keys are available until the user either "stops services" ("logs out") or an operator executes a reset (or cycles the module power).

When Starting Services, the user can choose either "FIPS mode" or "Non-FIPS mode". "Non-FIPS mode" is a functional superset of FIPS mode and enables non-FIPS approved cryptographic algorithms and key derivations.

Once services are started, users can carry out all cryptographic functions, import and export *protected*[6] keys (where enabled) over the network interface, generate keys (specifying if future export over the network interface is permitted) and random numbers, etc.

[5] 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 Enterprise, this interface line is wired to a keyswitch.

[6] 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.

5.1.3. Crypto Officer

In addition to being able to act as a *User* (as the crypto officer can also "start services" if a user has not already done so), a Crypto Officer can access the Smart Card interface in order to perform master key backup[7] 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. "Erasing All" keys 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").

5.2. Services and Critical Security Parameter (CSP) Access

5.2.1. CSP Definition

The following table describes the keys and CSP's stored or used by the module:

CSP Name	Description and /or Purpose	Type of Key or CSP	Storage Location
IMK (Image Master Key)	Protection of the SVK & AAK	Triple DES	SKS[8]
SMK (Storage Master Key)	Protection of User Keys	Triple DES	SKS
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 RSA public key	BBRAM, TDES encrypted by IMK.
DES MAC	Verify firmware integrity at power-on	DES MAC result	Stored in FLASH at end of firmware image.

[7] 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.

[8] The Secure Key Store (SKS) is a dedicated microcontroller 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.

5.2.2. 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 User and Operator Services are available to Crypto Officers.):

Role	Services	Notes	Access (RWX)
Operator	Modify Network Parameters	Although the operator can modify network parameters they do not become effective until the next restart of the module and an authenticated user has logged in.	W
Operator	View Firmware Version	-	R
Operator	View FIPS Mode	-	R
Operator	Execute Self Tests	-	X
Operator	View Audit Log	-	R
User	Log in.	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	Generate Key	RSA, DSA, DES, TDES, AES.	User Key - W
User	Sign	RSA, DSA	User Key - X
User	Verify	RSA, DSA	User Key - X
User	Encrypt/Decrypt	DES, TDES, AES	User Key - X
User	Get Random	PRNG (certificate #41)	X
Crypto Officer	Set module operational	AAK	AAK - X
Crypto Officer	Permanently disable all key export	Must be set before making module operational. (Also disables SMK backup/recovery.)	X

Crypto Officer	Disable key export via API		X
Crypto Officer	Create New User / Crypto Officer	Creates new smart card sets containing new authentication secrets.	AAK - X
Crypto Officer	Backup/Recover SMK	SMK (M of N components; La Grange interpolating Polynomial, one component per Smart Card, 2 of 4 to 9 of 9). SMK backup and recovery can be forbidden during initialization in order to confirm to the Digital Signature laws of some European states.	SMK R/W
Crypto Officer	Backup/Recover User Keys	User keys are copied to or from the module internal non-volatile store to or from smart cards. (All user keys stored within the module's non volatile store are encrypted with TDES under the SMK. Accordingly, all keys backed up to Smart Card are already encrypted with TDES under the SMK. Keys recovered from Smart Card must be encrypted by the module's *current* SMK or they cannot be decrypted and used by the module.) User Key backup and recovery can be forbidden during initialization in order to confirm to the Digital Signature laws of some European states,	User Keys - R/W
Crypto Officer	Zeroize All Keys	Zeroize ALL CSPs (except IMK, SSMK & SVR). Revokes all User and Crypto Officer Smart Cards. Returns module to "as delivered" state.	SMK, AAK & User Keys - X. (All zeroized)

6. Maintenance

With the exception of firmware updating, no other user maintenance of an module is possible. If a fault develops (including faults indicated by the self-test system), the module must be removed from service.

Repair of a module requires return to AEP Systems; no third party or site service is possible. Products based on module (for example, the AEP Keyper Enterprise) may potentially be repaired on the customer's site where the fault does not include module components (for example, SmartCard reader or display/keypad faults).

Please note, AEP is not aware of *any* mechanism which can recover customer's keys from a module 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.

6.1. Firmware Upgrade

User supplied firmware cannot be loaded into the module as it must be digitally signed by AEP, but field updates to more recent firmware revisions are possible.

AEP Enterprise CM's application firmware can be upgraded while on the module owner's site using the secure download process.

Note:

- ➲ If "FIPS-mode" operation of the module is required after firmware upgrade, the new firmware must be FIPS validated.

The download process replaces the factory-supplied application with new software. This downloaded firmware is digitally signed by AEP Systems and may also be encrypted.

Downloading requires a special AEP utility which runs on Microsoft Windows PCs. Customers with AEP support contracts can obtain both updates firmware and this utility from AEP support.

If the AEP Enterprise CM does not recognize the RSA digital signature applied to the update or if the downloaded firmware has an older version number than the firmware already loaded, it will reject the download and restart using its pre-update firmware:

Appendix A - Operator Guidance

A.1 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:

A.2 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.

If the product containing the module features its own tamper evident features and or temperature limit indicators these should also be inspected. (AEP Keyper products have tamper evident seals and have devices that indicate temperature limits have been exceeded).

A.3 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. After a short delay, this will be replaced by:

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

At this point, press 1 on the product keypad and insert the first SmartCard of a 2 card "SO[9]" set. You will be asked to enter the Card's PIN[10]; enter 11223344). (You can change this Card PIN later.)

[9] Cards used to identify *Users* and *Crypto Officers* are both termed "Security Officer Cards" in product documentation.
[10] The AEP Enterprise CM does not utilize or interpret these PINs directly. The PINs are required by the *SmartCards*. Their use is not validated as part of the AEP Enterprise CM FIPS 140-2 Level 4 validation. They supply additional "System-level" security.

After the first SO Card is initialized, you will be prompted to insert the second and to key in its PIN. (11223344.) When this card is also initialized, the creation of the first Crypto Officer is complete and you should proceed to "Go Operational" in order to complete the configuration and create any desired additional Crypto Officers and Users.

"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 both SO cards and keying in their PINs as prompted.

A.4 Operational State – Set Network Parameters

The module is designed to be incorporated in a network appliance. Before it can be used the IP network parameters must be set so that it can operate in your system. Setting the network parameters is an *operator* service and does not require authentication.

From the front panel menu select "1. Network", "1. Set", "1. HSM Config" and finally "1. IP Address". Key in a Class C IP address that is correct for your installation and press ENT to confirm it. If you wish you can also set the Network Net Mask via "1. Network", "1. Set", "1. HSM Config" and finally "2. Net Mask". Key in the relevant network mask and again press ENT to confirm.

A.5 Start Services in FIPS mode

From the front panel menu select "2. Security Officer". Insert a User or Crypto Officer SmartCard and enter its PIN when required. Remove the card when prompted. Select "4. Start Services".

A.6 Confirm FIPS mode operation

From the front panel menu select "1. Operator", "3. FIPS mode". The front panel display will now confirm the module is operating in FIPS mode by displaying "FIPS mode".

7. Document Configuration

Document details

File Name:	ACCE-EFIPSSecurityPolicy.doc
Document Title:	AEP Enterprise CM - 011126 FIPS 140-2 Security Policy
Document Revision No.:	8
Author:	AEP Networks
Approved By:	Paul Goffin
Revision Date:	10 May 2005