Ultra Electronics AEP's Advanced Configurable Cryptographic Environment (ACCE) v3 HSM Crypto Module

FIPS 140-2 Non-Proprietary Security Policy Issue 23

Table of Contents

1. Introduction

1.1. Scope

This document is the FIPS PUB 140-2 Security Policy for the ACCE v3.

It covers the following as used in the Ultra Electronics AEP Keyper Plus:

Hardware	2870-G1
Firmware	2r3, 2r4, 3r2, 3r3

Table 1- Hardware and Software Versions

The different firmware versions provide the following functionality:

2r3	Initial accreditation of ACCE v3
2r4	Enhanced smartcard security
3r2	Addition of remote management
3r3	Enhanced file cache

Table 2- Firmware Versions

1.2. Overview and Cryptographic Boundary

The *ACCE v3* is a *single user, multi-chip embedded* crypto-module. The FIPS PUB 140-2 cryptographic boundary is the metal case containing the entire ACCE v3 (below). The ACCE v3 is referred to in the remainder of this document as the 'module'.

Like its predecessors, the ACCE, ACCE-L3 and ACCE v2 modules, the ACCE v3 exists to provide cryptographic services to applications running on behalf of its user which communicate with it via a standard Ethernet interface using IP protocols. To implement these services, the module additionally requires a suitable power supply, Smart Card reader, USB port, digital display device, keypad and line drivers.

The ACCE v3 is usually sold embedded within a stand-alone "network appliance" Hardware Security Module [HSM] type product such as the Ultra Electronics AEP Keyper Plus (below).

The Keyper Plus 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

Table 3- FIPS 140-2 Security Requirements

[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, USB and Ethernet), control interface (Front panel and Ethernet), audit (serial port and Ethernet) and user data (Ethernet).

All ports and interfaces enter and leave the module via the ribbon cables as shown in the picture on the front page.

The following table describes the relationship between the physical connections available via the ribbon cables and their logical interfaces. (The module has no other electrical connections.)

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

Table 4- Mapping Physical and Logical Interfaces

The User Data (Ethernet) connection can

- accept plaintext data (to be encrypted or signed), encrypted keys and ciphertext data (to be decrypted)
- output plaintext data (output of a decrypt), encrypted keys (when enabled) and ciphertext data (output of an encrypt)

Logical distinctions between plaintext, encrypted keys and ciphertext are made in the Application Programming Interface (API).

[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.

The smart card port is used for front panel user authentication and key backup/recovery. Ethernet is used for remote authentication and key backup. Authentication and key backup/recovery cannot be run at the same time because a crypto officer must authenticate *before* they can utilize key backup or recovery functions. Remote operations also cannot be performed at the same time as front panel operations. So, user authentication and key backup/recovery operations are logically distinct.

2. FIPS and non-FIPS Operation

The ACCE v3 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. Application keys must be Zeroized on transition from FIPS to non-FIPS mode.

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

Appendix A contains instructions on how to transition from non-FIPS mode to FIPS mode.

2.1. Algorithms

Triple-DES and AES algorithms are carried out entirely in hardware using the SEC facility from the QorIQ processor. All Modular exponentiation used for RSA and DSA algorithms are carried out in the EXAR look-aside processor. All ECC algorithms are always carried out in the EXAR chip hardware. The EXAR chip collects entropy using an NDRNG. The NDRNG output is only used to seed the DRBG.

Triple-DES MAC is partially carried out in hardware (the Triple-DES part) and partially in firmware (converting that into the MAC)

Algorithm	Description	Hardware acceleration	Certificate number
SHS	SHA-1 SHA-224, SHA-256, SHA-384, SHA-512	Firmware only	#2255, #2782, #3384 and #3581
HMAC	SHA-224, SHA-256, SHA-384, SHA-512	Firmware only	#1671, #2138, #2686 and #2884
RSA	Key generation. Signature verification (PKCS#1, X9.31, PSS). 1024 to 4096 bit (in 64 bit steps).	EXAR 8203	#1384
RSA	Signature generation (PKCS#1, X9.31, PSS). 2048 to 4096 bit (in 64 bit steps).	EXAR 8203	#1384
ECDSA	Key generation. Signature generation. Curves: P-224, P-256, P-384, P-521	EXAR 8203	#470
ECDSA	Signature verification. Curves: P-192, P-224, P-256, P-384, P-521	EXAR 8203	#470
DSA	Signature verification 1024 bit modulus only	EXAR 8203	#813
Triple-DES	Key generation. Decrypt (TECB & TCBC). Key unwrapping (TECB & TCBC). Triple-DES MAC verification (vendor affirmed). 112 & 168 bit	QorIQ SEC	#1610
Triple-DES	Encrypt (TECB & TCBC). Triple-DES MAC generation (vendor affirmed). 168 bit.	QorIQ SEC	#1610
AES	Key generation using the DRBG. Encrypt, decrypt (ECB & CBC). 128, 192, 256 bit.	QorIQ SEC	#2684
DRBG	512 bit Hash DRBG (SP800-90A)	Firmware only	#434, #786 #1237 and #1387

Table 5 - FIPS approved cryptographic functions

Algorithm	Description
AES	Key wrapping[3] (ECB & CBC).
ECDH	Key agreement[4]. Curves: P-224, P-256, P-384, P-521
NDRNG	Hardware RNG used to seed the FIPS-approved DRBG
RSA Triple-DES	Key wrapping[5]. 2048 to 4096 bit keys (in 64 bit steps). Key wrapping[6] (TECB & TCBC).

Table 6 – Non-FIPS approved but allowed cryptographic functions

[3] AES (key wrapping; key establishment methodology provides between 128 and 256 bits of encryption security).
[4] ECDH (key agreement; key establishment methodology provides between 112 and 256 bits of encryption security; non-compliant less than 112 bits of encryption strength). No operations supported which are certifiable.
[5] RSA (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption security; non-compliant less than 112 bits of encryption strength).
[6] Triple-DES (key wrapping; key establishment methodology provides 112 bits of encryption strength).

Algorithm	Description
RSA	ISO 9796 signature generation and verification 1024 to 4096 bit keys (in 64 bit steps)
RSA	Signature generation (PKCS#1, X9.31, PSS). Key wrapping. 1024 to 1984 bit (in 64 bit steps).
AES	AES MAC[7] 128, 192, 256 bit
DSA	Parameter generation. Key generation. Signature generation. 1024 bit modulus only.
ECDSA	Key generation. Signature generation. Curves: P-192, secp256k1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP192t1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1
ECDH	Key agreement. Curves: P-192, secp256k1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP192t1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1
PBKDF2	Key derivation of Triple-DES keys (112, 168 bit)
PKCS#12	Key derivation of Triple-DES keys (112, 168 bit)
RIPEMD-160	Hash generation.
SEED	128 bit Key generation. Encrypt & decrypt. Key derivation of SEED keys. Key wrapping of SEED keys.
SPKM	Key derivation of Triple-DES keys (112, 168 bit)
SHA-1	Key derivation, padding and DSA parameter generation
Triple-DES	Key derivation
Triple-DES	Two key (112 bit) Encrypt (TECB & TCBC) Key wrapping (TECB & TCBC)[8] TDES MAC generation
XOR_BASE_AND_DATA	Key derivation

Table 7 – Non-FIPS cryptographic functions

[7] Not compliant with CMAC (NIST 800-38B)
[8] Triple-DES (key wrapping; key establishment methodology non-compliant less than 112 bits of encryption strength).

2.2. Key Generation

The module features a FIPS 140-2 approved deterministic random number generator (DRBG) complying to NIST SP800-90A. It is a SHA-512 HashDRBG which has a security strength of 256. This HashDRBG 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". The security strength of the HashDRBG is greater than or equal to the security strength of all keys the module can generate. All Application keys generated by the module rely on this DRBG, thus all Application keys *generated while in "FIPS mode"* are "FIPS keys".

2.2.1. Key Generation Detail

The HashDRBG is seeded and re-seeded using the random noise source on the EXAR 8203. The HashDRBG is reseeded on every 60Kbits of output. The seed value obtained from the random noise source is not used for any other purpose. The HashDRBG is not based on an encryption algorithm so does not use a seed key.

The key generation processes do not accept an external seed key. Intermediate key generation values are not output from the module on any key generation process.

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

Finally, all Asymmetric key pairs generated are subject to a pairwise consistency test.

2.2.2. Random Number Continual Self Tests

Please refer to 3.2. -3.2. Continual Tests.

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 all hardware and firmware components necessary for correct operation are self-tested.

An operator may initiate a self-test by initiating a reset. In addition a self-test of the random number generator can be initiated from the menu.

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

1. Boot-loader testing (assumes processor core and L1 instruction cache are operational):

   L1 instruction cache
   DRAM
   L2 cache

2. Application firmware:

   Integrity check of the Application Bootloader (ABL) with a CCITT32 CRC

   Integrity check of the Application with SHA-256.

3. Cryptographic Algorithms

Known Answer Tests of the following:

Algorithm	(Key) Size	Operation(s)
Triple-DES	112	Encipher and Decipher
AES	128	Encipher and Decipher
SHA-1		Digest
SHS (SHA-224, SHA-256, SHA-384, SHA-512)		Digest
RSA	2048	Sign and Verify
DSA	1024	Sign and Verify
ECDSA (P-256, secp256k1)		Sign and Verify
SEED	128	Encipher and Decipher
RIPEMD-160		Digest

DRBG (SHA-512)		Instantiation, Reseed, Generate and Zeroize
HMAC (SHA-224, SHA-256, SHA-384, SHA-512)		Generate

Table 8 – Cryptographic Self- Tests

The calculated output from the known answer tests is compared with fixed values which are in the code.

Any failure will cause the module to halt and display an error status message via the serial port. 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.

Any self-test failure suggests the hardware is faulty or has been incorrectly programmed. If a unit fails it should be returned to Ultra Electronics AEP.

Once the self-tests have successfully run the front panel shall display either “Important Read Manual”, “Secured 9860-1” or “Secured 9860-2”.

3.2. Continual Tests

The following are tested continually:

- DRBG: Continuous RNG test as specified in FIPS 140-2 Section 4.9.2. Each 512 bit block generated is compared to the previous 512 bit block. If they are the same then the DRBG is put into an error state and can no longer generate data.
- NDRNG: Continuous RNG test as specified in FIPS 140-2 Section 4.92. Each 32 bit block generated is compared to the previous 32 bit block. If they are the same then no data is returned and the NDRNG is left in an error state.
- DSA pair wise consistency test on key generation
- RSA pair wise consistency test on key generation.
- ECDSA pair wise consistency test on key generation

3.3. Firmware Load Test

The module can accept field updates to its internal firmware. These updates are digitally signed using the ECDSA algorithm and verified by a public key which is built into the module during factory commissioning. The image is encrypted using 128 bit AES.

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 ACCE v3 is an embedded module validated as meeting the requirements of FIPS PUB 140-2 level 4.

Any physical attempt to access the module's Critical Security Parameters (CSPs) will result in one of the following:

- If the CSP is stored in cleartext it will be zeroized
- If the CSP is wrapped by a storage key that storage key will be zeroized making the CSP inaccessible

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 zeroize all CSPs.

The epoxy hardness was tested at room temperature and at the high and low temperatures which would cause the active tamper (-25 to 80 degrees Celsius).

4.2. Physical Security Rules

The ACCE v3 will detect and respond to (by zeroising 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.

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 Ultra Electronics AEP for repair. In the Keyper Plus, this permanent power supply is provided by an internal battery.

5. Identity Based Authentication

5.1. Single User

The ACCE v3 supports multiple users but only one may have an active session at any time.

5.2. Role Authentication

The ACCE v3 has a set of read-only features for an unauthenticated user. Access to other features is partitioned by role such that a role has access to features required by that role but not to all features. A user must be authenticated as belonging to a role before using that role's features. In addition to the Unauthenticated User there are four authenticated roles; Operator, Crypto Officer, Security Officer and Remote User. Each user requiring authentication is authenticated using a Gemplus MPCOS compatible Smart Card reader/writer connected to the appropriate interface.

Authentication of an Operator, Crypto Officer or Security Officer requires a set of smart cards. A set of n cards are issued of which m must be presented to authenticate a user where:

$$2 <= n <= 9$$

$$2 <= m <= n$$

Cards are not interchangeable between sets.

Authentication states are not persisted in non-volatile storage. When a unit is power cycled the unit assumes no level of role authentication.

Authentication is required in both FIPS and non-FIPS modes.

To invalidate previously issued cards a new AAK should be generated.

Remote management uses the same role card authentication as local management. Additionally, when performing read-only activities remotely, which require no authentication locally, a single role-card is required.

5.3. Creating Role Cards

The ACCE v3 supports creation of sets of role cards. Sets of Security Officer cards are created when the module is initialised. Sets of Operator and Crypto Officer cards are issued by a user authenticated in the Security Officer role.

The procedure creates matched sets of cards which can only be used to authenticate for the issued role within the issued set of cards. Each card contains a unique number to tie the card to a set and to a role. The card also contains a 112 bit cryptographic secret (ASK).

5.4. Strength of Authentication Mechanism

In order to authenticate, a user must possess the appropriate 112 bit secret "key". This key is used to generate a 32-bit Triple-DES MAC over a random challenge. The probability that a random attempt at guessing the key will succeed is 1 in 2^{80} (112-bit Triple-DES has a security strength of 80).

There are two interfaces over which authentication takes place; the front panel and remote management.

First consider the front panel. A “brute force” attack on this key could be attempted once every 5 seconds. A sufficiently skilled attacker could develop equipment capable of conforming to the front panel interface definition and simulating the responses from the smart card module. In this way they could attack the 32-bit MAC value rather than the 112-bit key.

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 force in the "trial" MAC value, the time to regenerate the key value inside the ACCE and verify the MAC with it and the time to pass this data together with front panel menu data over a 9600 baud serial link. The attacker would not be able to bypass the sequence of commands in the firmware (as this is within the tamper proof boundary).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. This gives a maximum of 600 attempts in 1 minute.

For the second interface, Remote Management, a delay period is forced after each set of 5 consecutive failed attempts, this delay period doubles for each consecutive set of 5 failed attempts starting at 1 seconds and limited to a maximum of 20 minutes. Therefore the maximum number of failed attempts is 30 within 1 minute. We will take the worst case of 600 attempts in 1 minute via the front panel, and assume that the attacker is intelligent and will not retry a value that has failed. This results in the search space reducing by one on each attempt.

P(one of the first 600 attempts succeeding) = $\sum_{n=0}^{599} \frac{1}{(2^{32}-n)}$

The value of n is so tiny compared with 2^{32} that, as we don’t require an exact probability, we can disregard it.

So,

P(one of the first 600 attempts succeeding) $\approx \sum_{n=0}^{599} \frac{1}{2^{32}} = \frac{600}{2^{32}} \approx \frac{1}{1.4\times10^{7}}$ (i.e. 1 in 14 million)

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

If the user presents incorrect authentication data (the 32 bit MAC value) either on the front-panel or remotely the only feedback is that the authentication has failed. This failure information is displayed and also written to the audit log. No further information is revealed.

6. Roles and Services

6.1. Roles

The ACCE v3 supports the following Roles:

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

Table 9 - ACCE v3 Roles

The following sections describe what is allowed by users of a specific role. Unless explicitly stated the user cannot undertake any cryptographic operations, load or unload keys or access CSPs.

6.1.1. Unauthenticated User

The user may be accessing the unit either via the front panel or a local Ethernet connection.

The unauthenticated user role permits read-only access to the module's configuration including:

- Read-only viewing of the following configuration:
  - Battery Status
  - The FIPS mode
  - Date and Time
  - Network settings including addresses, masks and port numbers
  - Software versions and build date / time
  - Serial number
  - Audit Log
- View smart card details.

6.1.2. Remote User

A Remote User is accessing the unit via Ethernet on a separate physical port to the Unauthenticated User.

The role permits read-only access to the module's configuration including:

- Read-only viewing of the following configuration:
    - Battery Status
    - The FIPS mode
    - Date and Time
    - Network settings including addresses, masks and port numbers
    - Software versions
    - Serial number
    - Audit Log

6.1.3. Security Officer

The Security Officer role may perform all Unauthenticated User actions and is additionally authorised to:

- Import an AAK to a non-commissioned / unsecure unit*
- Set the global export option for a non-commissioned / unsecure unit*
- Secure a unit (commission a unit so it is capable of performing cryptographic operations)
- Switch between “FIPS mode” and “Non-FIPS mode”.
- Module management functions:
    - Enable the unit to go-online after a power cycle
    - Change the date / time
    - Change the network settings
    - Return the unit to its non-commissioned / unsecure state
    - Extract performance statistics
- Role Management functions:
    - Issue and clear Role cards
    - Backup the AAK and clear AAK cards
- Change smart card PINs

* These functions can be performed by an unauthenticated user but a Security Officer is required to subsequently secure the module so that the action is persisted.

6.1.4. Operator

The Operator role may perform all Unauthenticated User actions and is additionally authorised to:

- Turn the unit on or off-line. An on-line unit is available for cryptographic operations across the network interface. An off-line unit will not perform cryptographic operations across the network interface.
- Change smart card PINs

6.1.5. Crypto Officer

The Crypto Officer role may perform all Unauthenticated User actions and is additionally authorised to:

- List the details of the keys held in the module
- Back-up / restore and delete application keys
- Generate / back-up / restore and delete the SMK.
- Change global options on which API operations are allowed, e.g. key generation or key export.
- Enable / disable support of non-Suite B algorithms.

- Back-up / restore of the crypto options to smartcard.
- Change smart card PINs

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 (Footnote - How Zeroized)
IMK (Image Master Key)	Protection of the SVK, SKEK & AAK	128 bit AES	SKS[9]
ISMK (Internal Storage Master Key)	Protection of Application Keys stored internally in Flash	256 bit AES	SKS[9]
SMK (Storage Master Key)	Protection of Application Keys backed up to smart cards	192 bit Triple-DES or 256 bit AES	SKS[9]
AAK (Authentication String)	Authentication of Roles	112 bit secret random value.	Black Store encrypted by IMK[10]
Application Keys	Encryption/Decryption, or Signatures	Triple-DES, AES, DSA, RSA, ECDSA	encrypted by SMK[Error! Bookmark not defined.8]
FSVK (Factory Software Verification Key)	Verification by the bootloader that factory images for programming originate from Ultra Electronics AEP.	256 bit ECDSA	Compiled into ACCE 3 BBL bootloader[11]
SVK (Software Verification Key)	Verify Firmware Downloaded to Module	256 bit ECDSA	Flash encrypted by IMK[108]
SKEK (Software Key Encryption Key)	Decryption of Software Encryption Key (SEK).	128 bit AES	Flash encrypted by IMK[108]
Firmware hash	Verify firmware integrity at power-on	SHA-256 hash	Stored in FLASH at end of firmware image[12]
DRBG State	DRBG State	V and C as defined in NIST SP800-90A	RAM[13]
Smartcard ID	Non-repudiation	16 numeric characters	Smartcard (read only, set at card manufacture)[14]
Smartcard PIN	Authentication of Roles	4-8 numeric characters	Smartcard (in write only memory)[1412]
RMPK (Remote Management Private Key)	Issuing X.509 certificates and establishing TLS tunnels for Remote Management.	384 bit ECDSA	Black Store encrypted by ISMK[108]

Table 10 - Critical Security Parameters

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

[10] Effectively zeroized when the key encrypting the CSP is itself zeroized.

[11] Only the public key is held within the ACCE3 so does not need zeroizing. The private key is securely held within Ultra Electronics AEP's List-X room.

[12] Is not zeroized. There to protect the integrity against accidental corruption so does not need to be zeroized on tamper.

[13] Held in 'red memory' which is overwritten with zeroes on a tamper or power-down.

[14] Protected by the GemPlus SmartCard

6.2.2. Services and Access

The following table summarizes the CSPs accessed by the various roles in utilizing the module's services.

"Unauth" refers to Unauthenticated User accessing the unit either via the Front Panel or Ethernet over the local port. Services available to Unauthenticated Users are also available to Operators, Crypto Officers and Security Officers.

"Remote" refers to Users accessing configuration via the Remote Ethernet port.

"All services are carried out in FIPS mode unless otherwise stated.

Some services can be executed concurrently with other services. The following table contains a concurrency column. Services marked as 'Yes' can be run at the same time as cryptographic operations on the Ethernet port. Additionally these services may be performed at the same time as any other services:

- Audit may be extracted at any time
- Status may be extracted or firmware may be updated when the ACCE is online

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Unauth	View Network Settings	-	Y	No CSPs accessed
Remote	First remote access	When a TLS connection to a Remote User does not already exist to establish a new TLS connection.	Y	RMPK - X
Remote	View Network Settings		Y	Smartcard PIN, AAK - X
Unauth	View Battery Status	-	Y	No CSPs accessed
Remote	View Battery Status	-	Y	Smartcard PIN, AAK - X
Unauth	View Date / Time	-	Y	No CSPs accessed
Remote	View Date / Time	-	Y	Smartcard PIN, AAK - X
Unauth	View Software Versions and Build Date / Time	-	Y	No CSPs accessed

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Remote	View Software Versions	-	Y	Smartcard PIN, AAK - X
Unauth	View FIPS Mode	-	Y	No CSPs accessed
Remote	View FIPS Mode	-	Y	Smartcard PIN, AAK - X
Unauth	View HSM Serial Number	-	Y	No CSPs accessed
Remote	View HSM Serial Number	-	Y	Smartcard PIN, AAK - X
Unauth	View Card Details	-	Y	Smartcard ID - R
Crypto Officer or Security Officer	View Card Details	Details specific to that Role.	Y	Smartcard ID - R
Unauth	Execute Self Tests	-	N	No CSPs accessed
Unauth	View Audit Log	-	Y	No CSPs accessed
Remote	View Audit Log	-	Y	Smartcard PIN, AAK - X
Unauth	View Status (Output Status)	-	Y	No CSPs accessed
Operator, Crypto Officer or Security Officer	Authenticate	An authentication secret is derived from the AAK and the User ID values. User responds to a random challenge by calculating aTriple-DES MAC with his copy of this secret and returning the result.	Y	Smartcard PIN, AAK - X
Operator, Crypto Officer or Security Officer	Change PIN	Change User smart card PIN. Requires knowledge of the current PIN.	Y	Smartcard PIN - W

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Operator	Generate Key	RSA, ECDSA, AES, Triple-DES.	Y	Application Keys – W
Operator	Sign	RSA, ECDSA	Y	Application Keys – X
Operator	Verify	RSA, DSA, ECDSA.	Y	Application Keys – X
Operator	Encrypt / Decrypt	Triple-DES, AES.	Y	Application Keys - X
Operator	Key (un)wrap	Triple-DES, AES, RSA.	Y	Application Keys – W, X
Operator	Hash data	SHS.	Y	No CSPs accessed
Operator	HMAC	SHA-224, SHA-256, SHA-384, SHA-512	Y	Application Keys – X
Operator	HMAC Verify	SHA-224, SHA-256, SHA-384, SHA-512	Y	Application Keys – X
Operator	MAC	Triple-DES	Y	Application Keys – X
Operator	MAC Verify	Triple-DES	Y	Application Keys – X
Operator	Key Agreement	ECDH (compliant curves)	Y	Application Keys – X
Operator	Get Random	DRBG.	Y	No CSPs accessed
Operator	Reseed DRBG	DRBG.	Y	No CSPs accessed
Operator	Set module on-line	AAK.	N	Smartcard PIN, AAK - X
Security Officer	Secure a unit	Writes the encrypted AAK to BlackStore so that only role cards issued with this AAK may now use services.	N	AAK - W
Security Officer	Unsecure a unit	Zeroizes the ISMK and SMK. Returns the module to the non-commissioned Unsecure state.	Y	ISMK – W, SMK – W (Zeroized)

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Security Officer	Import an AAK	Can be performed by an unauthenticated user but requires a Security Officer to persist the import by securing the unit.	N	AAK-W
Security Officer	Permanently disable all key export	(Also disables SMK backup/recovery.) Can be performed by an unauthenticated user but requires a Security Officer to persist the setting by securing the unit.	N	No CSPs accessed
Security Officer	Modify Network Settings	-	N	No CSPs accessed
Security Officer	Set the FIPS mode	-	Y	No CSPs accessed
Security Officer	Set auto on-line	Allow a unit to automatically go on-line after a power cycle or reset. Auto-online must not be enabled in FIPS mode.	Y	No CSPs accessed
Security Officer	Set the date / time	-	Y	No CSPs accessed
Security Officer	View performance statistics	-	Y	No CSPs accessed
Security Officer	Enable / disable Remote Management	-	Y	No CSPs accessed
Security Officer	Export Remote Management certificate	Generate the RMPK if it does not already exist and generate an X.509 certificate using the RMPK.	Y	RMPK – WX
Security Officer	Generate a new RMPK	-	Y	RMPK – W
Security Officer	Issue Role Cards	Creates new Operator or Crypto Officer smart card sets (m of n) containing new authentication secrets on 2<=n<=9, 2<=m<=n Smart Cards.	Y	AAK – X
Security Officer	Clear Role / AAK Card	-	Y	AAK – X
Security Officer	Backup AAK	AAK (m of n components; XOR, one component per Smart Card, 2<=n<=9, 2<=m<=n).	Y	AAK – W

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Crypto Officer	Output key summary	Outputs the number of Application keys stored in the module (by algorithm, key size, private / public,) to the serial port.	Y	No CSPs accessed
Crypto Officer	Output key details	Outputs per key stored to the serial port details of label, algorithm, size, FIPS key, policy and usage rules.	Y	No CSPs accessed
Crypto Officer	Generate SMK		Y	SMK - W
Crypto Officer	Backup SMK	SMK (m of n components; La Grange interpolating Polynomial, one component per Smart Card, 4<=n<=9, 2<=m<=n). SMK backup can be disabled during initialisation in order to confirm to the Digital Signature laws of some European states.	Y	SMK - R
Crypto Officer	Recover SMK	SMK (m of n components; La Grange interpolating Polynomial, one component per Smart Card, 4<=n<=9, 2<=m<=n). SMK recovery can be disabled during initialization in order to confirm to the Digital Signature laws of some European states.	Y	SMK - W
Crypto Officer	Backup Application Keys	Application keys are exported from the module to smart cards or USB. Keys stored in the module are decrypted with the ISMK, re-encrypted with the SMK and written to the smartcard or USB. Application Key backup can be disabled during initialisation in order to confirm to the Digital Signature laws of some European states,	N	Application Keys – W SMK – X ISMK - X
Crypto Officer	Recover Application Keys	Application keys are imported to the module's internal non-volatile store from smart cards or USB. Smartcard or USB keys are decrypted with the SMK, re-encrypted with the ISMK and written to the modules internal non-volatile store. Application Key recovery can be disabled during initialisation in order to confirm to the Digital Signature laws of some European states,	N	Application Keys – W SMK – X ISMK - X

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Crypto Officer	Delete All Application Keys	Delete All Application Keys	N	Application Keys – W
Crypto Officer	Enable or disable key import via API	Allows/disallows key import (wrap) via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable key export via API	Allows/disallows key export (unwrap) via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable Asym key pair generation for use with API	Allows/disallows RSA/ECDSA key pair generation via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable Sym key generation for use with API	Allows/disallows AES/Triple-DES key generation via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable Sym key derivation for use with API	Allows/disallows AES/Triple-DES key generation via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable signature generation for use with API	Allows/disallows RSA / ECDSA signing. A signing via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable verification for use with API	Allows/disallows DSA / RSA / ECDSA signature verification via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable MAC generation for use with API	Allows / disallows AES / Triple-DES MAC Generation via the API	Y	No CSPs accessed
Crypto Officer	Enable or disable MAC verification for use with API	Allows / disallows AES / Triple-DES MAC Verification via the API	Y	No CSPs accessed

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Crypto Officer	Enable or disable encryption /decryption for use with API	Allows/disallows AES/Triple-DES encryption or decryption via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable Asym key deletion for use with API	Allows/disallows DSA/RSA/ECDSA keys to be deleted via the API.	Y	No CSPs accessed
Crypto Officer	Enable or disable Sym key deletion for use with API	Allows/disallows AES/Triple-DES keys to be deleted via the API.	Y	No CSPs accessed
Crypto Officer	Enable / disable the use of non-Suite B functions for use with API	Allows/disallow non-Suite B algorithms to be used via the API. A 'disable' overrides all enables elsewhere (e.g. if non-Suite B is disabled, DSA/RSA signing is not allowed even if asymmetric signing is enabled) An 'enable' does not override operations which have been disabled.	Y	No CSPs accessed
Crypto Officer	Backup settings	The above enable/disable settings can be saved to smart card.	Y	No CSPs accessed
Crypto Officer	Recover settings	The above enable/disable settings can be restored from smart card.	N	No CSPs accessed
Operator	Update firmware	Update the firmware: the firmware downloads' signature is verified and the firmware decrypted. If the firmware is older than the current firmware the download is rejected. The unit must be put on-line by an Operator.	Y	Firmware hash - W

Table 11 - Services accessing CSPs in FIPS mode

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Operator	Non FIPS mode: Encrypt	Two key Triple-DES.	Y	Application Keys - X

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Operator	Non FIPS mode: Key wrap	Two key Triple-DES.	Y	Application Keys – W, X
Operator	Non FIPS mode: MAC	Two key Triple-DES, AES.	Y	Application Keys – X
Operator	Non FIPS mode: Key Agreement	ECDH (non-compliant curves)	Y	Application Keys – X
Operator	Non FIPS mode: Derive Key	Triple-DES (SPKM mechanism) and XOR based key derivation.	Y	Application Keys – W, X
Operator	Non FIPS mode: Generate Key	Triple-DES, DSA, SEED, ECDSA (secp256k1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP192t1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1).	Y	Application Keys - W
Operator	Non FIPS mode: Encrypt / Decrypt	Triple-DES, SEED.	Y	Application Keys - X
Operator	Non FIPS mode: Key (un)wrap	SEED	Y	Application Keys – W, X
Operator	Non FIPS mode: Key gen, encryption and decryption in CBC mode	Triple-DES – PKCS#5 (PBKDF2)	Y	Application Keys – W, X

Role	Services	Notes	Concurr-ent Y(es) / N(o)	Access (RWX)
Operator	Non FIPS mode: Sign	RSA signature with ISO 9796 padding. ECDSA (secp256k1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP192t1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1)	Y	Application Keys - X
Operator	Non FIPS mode: Derive Key	Triple-DES (PKCS#12 mechanism). PKCS#12 in non FIPS mode only.	Y	Application Keys – W, X
Operator	Non FIPS mode: Derive Key	ECDH (secp256k1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1, brainpoolP192t1, brainpoolP224t1, brainpoolP256t1, brainpoolP320t1, brainpoolP384t1, brainpoolP512t1).	Y	Application Keys – W, X
Operator	Non FIPS mode: Derive Key	SEED.	Y	Application Keys – W, X
Operator	Non FIPS mode: Hash data	RIPEMD-160.	Y	No CSPs accessed

Table 12 – Additional services accessing CSPs in Non FIPS mode

6.2.3. Handling of CSPs

Plaintext keys, plaintext key components, plaintext authentication data and other unprotected CSPs are not input to or output from the module. As a result we do not need a trusted path for these data.

Control inputs are received through the FRONTPANEL or ETHERNET interfaces but only once authentication has been done. Firmware upgrades are sent encrypted and signed through the Ethernet interface. Status output is sent out of the module through the SERIAL interface.

Plaintext private and secret keys are not input to or output from the module. The memory in which the application keys are stored is not exposed through any interface so cannot be written to or read without breaking the tamper proof boundary. All private and secret application keys are stored encrypted under the ISMK. The FRONTPANEL, ETHERNET and API do not allow any keys to be modified or substituted.

Key processes and data paths

It is essential that all output data paths are physically or logically disconnected from the processes which handle plaintext keys. The output data paths which need to be considered are Ethernet, smartcard, USB and front panel.

Key generation

All key generation is controlled by the Crypto Kernel module. The Crypto Kernel itself does not send data to any of the output paths and the Crypto Kernel interface ensures that no plaintext key data is revealed to any calling modules. As a result, all output data paths are logically disconnected from the key generation process.

Import and export of encrypted application keys over the Ethernet interface can be done by the User (once the Operators have enabled the Ethernet interface i.e. the unit has been set online).

Electronic key entry and output

No electronic key entry processes output plaintext key data.

Using automated key transport

Encrypted application keys belonging to the user can be imported to and exported from the module over the Ethernet interface. These processes are controlled by the Crypto Kernel module. The Crypto Kernel itself does not send data to any of the output paths and the Crypto Kernel interface ensures that no plaintext key data is revealed to any calling modules. As a result, all output data paths are logically disconnected from this electronic key entry process.

Import and export of encrypted application keys over the Ethernet interface can be done by the User (once the Operators have enabled the Ethernet interface i.e. the unit has been set online).

Using manual key transport

Key backup and recovery of the user's encrypted application keys can be done from smartcard, USB or Ethernet. Ethernet can only be used for key backup. Key backup and recovery of the SMK in component form can be done from a set of smartcards (a minimum of 2 smartcards are required).

These operations are authorised by the Crypto Officers. These operations can only be done when the Ethernet interface for data input and output has been disabled (unit has been set offline). Only one operation at a time can be done through the user interface (which includes the smartcard, USB and front panel). All output data paths are logically disconnected from these electronic key entry processes.

Manual key entry and output

The module does not accept manually-entered cryptographic keys.

Key zeroization

The key zeroization process is run on a hardware tamper event as a separate thread and does not access any of the output data paths. All output data paths are logically disconnected from the key zeroization process.

7. Maintenance

The ACCE v3 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 ACCE v3 requires return to Ultra Electronics AEP; no third party or site service is possible.

Please note, Ultra Electronics AEP is not aware of *any* mechanism which can recover customer's keys from an ACCE v3 without either access to the Crypto Officer authentication Smart Cards or key backup Smart Cards. Ultra Electronics 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 Security Officer

On delivery the module should be in "Unsecured 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):

" Unsecured 9860>"
"1. Issue SO 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[15]. 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.)

Multiple sets of SO cards should be created now as none can be issued once the unit has been secured.

When all cards have been initialized, the creation of the Security Officer card set is complete and you should proceed to "Secure" in order to complete the configuration and create any desired additional role cards.

"Secure"

Now the first Security Officer exists, the module should be made operational by selection menu item "3.Secure". The Security 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 Security Officer has been authenticated the Keyper will prompt for the SMK type, network configuration, FIPS mode and the time and date (to set up the real time clock).

Finally the Keyper reboots to ensure that the new network settings are used.

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

When Secure the Security Officer should change their PIN using the 'Change PIN' menu option.

Secured State

Creating the First User

Select the ”7.Role Mgmt” menu option. The Security 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 Security Officer has been authenticated select the menu option “1.Issue Cards”. At this point, Select the type of card (CO or OP), 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[16]. 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.)

Set on-line in FIPS mode

FIPS mode is the default.

From the front panel menu select “1.Set Online”. The Operator 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 “4.HSM Info”, press ENT, select “2.FIPS Mode” and press ENT. The front panel display will now confirm the module is operating in FIPS mode by displaying “FIPS Mode On”.

Setting FIPS mode on

To transition from non-FIPs mode to FIPs mode select “3. Set FIPS mode” on the front panel. The selection must be authorised by M of N Security Officers smartcards. The display will now show:

“FIPS Mode Off

Enable?”

Pressing ENT will change the mode to FIPS mode.

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

Appendix B Security strengths

Introduction

This section presents the security strengths of all keys which can be generated by the module.

Keys

Algorithm	**Key size**	**Bits of security**
SHA-512 HashDRBG	-	256
AES	128	128
	192	192
	256	256
2-key Triple-DES	112	80
3-key Triple-DES	168	112
DSA	1024 (160 bit subprime)	80
RSA	1024 - 1984	80
	2048 - 3008	112
	3072 - 4096	128
ECC	192	80
	224	112
	256	128
	384	192
	521	256

Table 13 - Key Strengths

AAK	Adaptor Authorisation Key, used to derive the ASK
ACCE	Advanced Configurable Cryptographic Environment
ASK	Adaptor Sub Key. Challenge \ response for authorising role cards.
CO	Crypto Officer
EXAR	The cryptographic co-processor in the ACCE
FSVK	Factory Software Verification Key, Verification by the bootloader that factory images for programming originate from Ultra Electronics AEP.
HSM	Hardware Security Module
IMK	Initialisation Master Key, Protection of the SVK, SSMK, SKEK, SSEK & AAK
ISMK	Internal Storage Master Key, Protection of Application Keys stored internally in Flash
MPCOS	Type of smartcard manufactured by Gemalto supported by the ACCE
OP	Operator
QorIQ	The processor in the ACCE running the application software
RMPK	Remote Management Private Key for creating TLS tunnels for Remote Management
RPK	Recovery Public Key
SKEK	Software Key Encryption Key, Decryption of Software Encryption Key (SEK).
SMK	Storage Master Key, Protection of Application Keys backed up to smart card or USB
SVK	Software Verification Key, Verify Firmware

	Downloaded to Module
SO	Security Officer
USB	Universal Serial Bus

Table 14 - Glossary