BALTIMORE

Baltimore ACCE Family

010387 FIPS 140-1 Security Policy

Table of Contents

1. Introduction

This document describes the FIPS PUB 140-1 view of the Baltimore ACCE family security policies.

1.1. The Baltimore ACCE Family

The *Baltimore Advanced Configurable Crypto Environment* (see front cover picture) is a "multi-chip embedded" cryptographic module.

This module is available in two physical forms:

1. (The ACCE) is contained within a tamper resistant and detecting enclosure certified as meeting FIPS PUB 140-1 level 4.
2. (The ACCE-L3) is contained within an epoxy resin enclosure certified as meeting FIPS PUB 140-1 level 3. The ACCE-L3 also incorporates power and temperature detection and response mechanisms certified as meeting FIPS PUB 140-1 level 4.

➲ The cover picture is of an ACCE. The ACCE-L3 is similar but does not have a flexible cable connector.

All ACCE/ACCE-L3 variants are *single user* modules i.e.; they provide cryptographic services to exactly *one* user. This *single user* is an embedded firmware application which can only be generated and loaded by Baltimore or licensed OEMs (FIPS approved Cryptographic techniques (see Section 5: Identity Based Authentication for details) ensure this. Note: user code cannot be loaded dynamically, though authenticated field updates are possible). ACCE/ACCE-L3s do not allow this *single user* to undertake crypto officer functions; Crypto Officers are differently authenticated and have access to an independent data interface (dedicated serial port assumed to be connected to a display, keypad & SmartCard reader.).

ACCE/ACCE-L3's include a commercial RISC (Reduced Instruction Set Computing) microprocessor which manages and/or undertakes the cryptographic services provided by the module. They also include dedicated hardware modules for carrying out common cryptographic functions (modular exponentiation and symmetric algorithm operations).

1.2. The SureWare Keyper

The *Baltimore SureWare Keyper* is an example of Baltimore product containing the ACCE combined with an application (the *single user* of the ACCE; in this case the "SureWare Keyper Professional" application*)* to provide ACCE cryptographic functions such as Encrypt / Decrypt, Hash, MAC, Sign, Verify, Generate Keys, etc. to a standard (network) interface.

The SureWare Keyper physically consists of an ACCE module, a SmartCard interface unit, case, keypad, display, battery, power supply unit and the network interface. (The battery maintains internal storage keys during power-off state; the unit is not battery powered.)

The SureWare Keyper is designed to be connected directly to a host computer, **not** to a public network. In operation, plain text / cypher text and end user commands all pass over the same interface – the SureWare Keyper does not enforce data separation at that level. (Thus its operation is similar to an embedded "crypto PCIcard", not a Virtual Private Network (VPN) device. However, unlike a PCI card, the SureWare Keyper has its own SmartCard Reader contained in the box and can easily be disconnected from the host computer for secure storage when not in use.)

Although technically possible, Baltimore does not currently offer the SureWare Keyper with theACCE-L3 cryptographic module (only the "Level 4" ACCE). If a "Level 3" SureWare Keyper is of interest, please contact your local Baltimore sales office.

1.3. SureWare PCI

The Baltimore SureWare PCI card is an example of the application of the ACCE-L3. Functionally identical to the SureWare Keyper, but in a PCI card package, the SureWare PCI provides a highly secure key protection solution where "single box" operation is required.

2. Non-FIPS Operating Modes

2.1. General

The Baltimore ACCE/ACCE-L3 family offer a range of cryptographic facilities and mechanisms, subject to factory build options.

When operated in FIPS mode, the ACCE is certified to operate at FIPS PUB 140-1 level 4 after the initialisation process is completed (Initialisation generates or imports the data used to authenticate Crypto Officers.) The ACCE-L3 is similarly certified, but to FIPS PUB 140-1 level 3.

2.2. Support of non-FIPS algorithms

Where build options permit, non-FIPS modes operation for cryptographic functions or non-FIPS approved algorithms (where non-FIPS approved algorithms are provided) may also be selected.

Choice of FIPS/non-FIPS cryptographic functions or algorithms is determined by an API (Application Programming Interface) parameter and is selected on a command-by-command basis by the embedded application (*i.e. the user*).

2.3. Further non-FIPS operation

In addition to the above, two (or more) Authenticated Crypto Officers acting together may enable further non-FIPS modes of operation. These modes may enable (for example) the user to export plain text private keys via the data interface in order to support legacy applications.

A significant non-FIPS service is the ability of Crypto Officers to “backup” protected (i.e. encrypted) user keys to Smart Cards via the Smart Card port. (This function can be prohibited at initialisation on “SV” variants.)

3. Physical Security

3.1. Introduction

The ACCE is contained within an embedded module certified as meeting the requirements of FIPS PUB 140-1 level 4. Similarly, the ACCE-L3 is contained within an embedded module certified as meeting the requirements of FIPS PUB 140-1 level 3 (+EFP).

A cryptographic key hierarchy headed by the Storage Master Key (SMK) protects security relevant data within the ACCE/ACCE-L3. Another similar cryptographic key hierarchy headed by the Image Master Key (IMK) protects the operation of the ACCE/ACCE-L3 itself and permits authorised firmware field updates. (Authorised updates must be FIPS validated to retain FIPS-certified operations).

For the ACCE, the module surrounding the cryptographic processor (and associated memory, cryptographic acceleration devices, etc.) provides a tamper-detecting envelope, within an opaque resin coating and an outer metal case. Attempts to access the cryptographic processor and/or associated devices (including cutting, chemically dissolving or removing battery power as this enables the protection circuitry) cause the module to halt and to zeroise all plain text (secret or private) keys (user keys and the two storage master keys – the SMK & IMK). The ACCE-L3 features an opaque epoxy resin coating which deters attempts to access the module, but does not feature the detection and response mechanisms of the ACCE. The ACCE-L3 does, however, zeroise keys as described above if battery power is removed.

For all ACCE/ACCE-L3s, once the IMK has been zeroised, on-site recovery (including any attempt to re-install firmware) of the module is impossible. The module must then be removed from service (it will be non-functional) and we recommend that it is returned to Baltimore for repair.

If the ACCE/ACCE-L3 is taken beyond its operational temperature range, it halts and zeroises all plain text (secret or private) keys and the SMK. On return to normal temperature, the unit can be restarted and (where the user application provides this service as in SureWare Keyper) keys can be re-entered from backup (if such backups exist).

Note:

- Latest (i.e. **all** except the obsolete "ACCE-G1") build variants feature an additional measure. If the ACCE is taken beyond its *storage* temperature range the IMK is also zeroised (in addition to the halting and zeroisation of all other plain text secret or private keys that will have already occurred as a result of exceeding the operational temperature range). Note also, **all** ACCE-L3 modules provide this feature. As described above, once zeroisation of the IMK has occurred, the ACCE/ACCE-L3 cannot be recovered on-site.

3.2. Physical Security Rules

The unit must be disconnected and removed from service in the following instances:

a) The battery voltage indicator is showing low state. (Where supplied as in the SureWare Keyper)

b) There are signs of physical tamper, i.e. any security labels (where fitted) have been damaged, holes have been drilled, or there is evidence of attempts to gain entry to the unit.

c) A power module other than the module approved has been connected.

d) It is known that the unit has been subjected to temperatures outside the specified storage temperature range.

e) There is evidence of chemical attack, i.e. corrosion or discoloration.

We recommend that the unit is returned to Baltimore for inspection / investigation / repair where any of the above occur.

4. Roles and Services

ACCE/ACCE-L3s support (single) User and Crypto Officer Roles. Two variations of software functionality exist (BE and SV) these variations only affect the Crypto Officer role as shown below.

4.1. User Role

(User role services are accessed by a single user; the embedded application.)

Services Available:

- Encrypt/Decrypt.
- Sign/Verify Signature
- Hash/Verify Hash
- MAC/Verify MAC
- Generate Symmetric Key.
- Generate Asymmetric Key Pair.
- Export/Import Protected Key.
- Store Protected Key.

The user has no direct access to Security Parameters. (i.e., the user utilises keys by label & function. The user does not access the actual *value* of a key.)

4.2. Crypto Officer Role

The Crypto Officer accesses the ACCE/ACCE-L3 via the administration interface. This interface requires a display panel, keypad and SmartCard reader (as provided in the SureWare Keyper). The Crypto Officer cannot carry out user functions.

The Crypto Officer can:

- Generate a new SMK.
- Create a new Crypto Officer SmartCard set.
- Enable/Disable non-FIPS operation modes (requires at least two Crypto Officers).

In BE variants, the Crypto Officer can:

- Export the SMK (in n from m component form).
- Import a new SMK (in n from m component form).
- Generate a new SMK.

- Export/Import protected user keys. (non-FIPS operation)

In BE variants, the Crypto Officer has access to the SMK and to all user protected keys.

In SV variants, the Crypto Officer can (at initialization):

- Prevent all access to the additional crypto officer functions available permanently to BE variants.

In SV variants, once the Crypto Officer has disabled these functions, no Crypto Officer has access to the SMK or to any user protected keys. (The functions cannot be re-enabled except by re-initialisation, which generates a new SMK and hence causes all user keys to become inaccessible (They are encrypted by a key which no longer exists.).)

5. Identity Based Authentication

5.1. User

There is a single user of the ACCE/ACCE-L3 Application Program Interface (API). This is the companion embedded application. This application is linked to the ACCE/ACCE-L3 at factory build time and the resultant firmware image is digitally signed. This digital signature is verified during construction and then stripped by the loader firmware (i.e. the digital signature is not stored). This firmware then calculates a DES MAC (as defined in ISO/IEC 9797:1994 & FIPS PUB 113) of the user application which it stores. Every time an ACCE/ACCE-L3 is restarted (i.e. power on) or reset, the MAC is recalculated and compared with the stored version. In the event that an ACCE/ACCE-L3 is unable to verify this MAC, it will refuse to operate and should be returned to Baltimore for reloading/repair.

5.2. Crypto Officers

The ACCE/ACCE-L3 identifies and authenticates their Crypto Officers via a challenge response protocol to a device capable of responding to a formatted random challenge. Correct response depends on knowing a 56 bit shared secret.

The ACCE/ACCE-L3 provides software support for an attached SmartCard reader/writer and display panel/keypad for user messages. Compatible SmartCard readers and a combined display/keypad are built into Baltimore products such as the SureWare Keyper and provided as hand-held units for the SureWare PCI.

The application end user must ensure that proper procedures are followed to protect the Crypto Officer SmartCards and their PINs from improper use or disclosure.

6. Security Data

The following are security data.

- Storage Protection Keys:

  IMK (Image Master Key), SMK (Storage Master Key)

- Crypto Officer Authentication Keys:

  These are derived (proprietary, non-FIPS derivation) 56 bit secrets. The fundamental secret from which they are derived is stored in *protected* form (for properties of "protected" see note below in "user keys" definition) in non-volatile RAM.

- User Keys:

  All user keys. (when unencrypted)

  Notes:

  - All user keys are *protected.*

    Protected keys are always encrypted (DES CBC under the SMK) except when they are decrypted for use. These "working copy" Plain Text instances of *protected keys* can only exist within the regions of the ACCE which are actively zeroised on tamper.

  - The *user application* cannot access plain text keys. (For example, the software interface providing functionality such as "get key value" simply does not exist.)

  - By definition, the storage protection keys, (the SMK and IMK) always exist in plain text form. The SMK *never* leaves the protected physical area except via the Crypto Officer interface in component form when required by authenticated Crypto Officers (note this can be prevented in SV variants). The IMK can never be exported.

7. Firmware Loading

7.1. Factory Firmware Download and Key Initialisation

Firmware is downloaded into ACCE/ACCE-L3s (namely the application, the secure download facility itself and software to generate / set up the ACCE/ACCE-L3's Storage Protection Keys, ACCE/ACCE-L3's Firmware Download Keys and Initialisation Keys) during factory initialisation. This firmware is signed with a factory key and downloaded to ACCE/ACCE-L3s on secure premises on Baltimore's site, supervised by the Baltimore Security Officer.

ACCE/ACCE-L3s rejects improperly signed firmware. The initial load facility is disabled by the ACCE/ACCE-L3s on receipt of the secure download firmware and re-enabled should an ACCE/ACCE-L3 be the subject of an actual tamper (breech of the tamper resistant mesh).

Should an ACCE/ACCE-L3 be the subject of an actual tamper (and thus, zeroisation of the IMK), a challenge/response mechanism is invoked prior to the firmware reload. This makes use of a public/private key encryption mechanism and a large random number. As this mechanism requires knowledge of Baltimore's private key, it can only be undertaken on Baltimore's secure premises.

7.2. Firmware Upgrade

ACCE/ACCE-L3s application firmwares can be upgraded while on the application 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 Baltimore and may also be encrypted.

If the signing keys are not recognised by an ACCE/ACCE-L3s, it will reject the download and restart using its existing firmware.

8. Maintenance

No user maintenance of an ACCE/ACCE-L3 is possible. If a fault develops (including faults indicated by the self-test system), the ACCE/ACCE-L3 must be removed from service.

Repair of an ACCE/ACCE-L3 requires return to Baltimore, no third party or site service is possible. Products based on the ACCE/ACCE-L3 (for example, the SureWare Keyper or SureWarePCI) may potentially be repaired on the customer's site where the fault does not involve ACCE/ACCE-L3 components (for example, SmartCard reader or display/keypad faults).

Configuration Control of this Document

Document details

File Name:	FIPSSecurityPolicy.doc
Document Title:	Baltimore ACCE Family - 010387 FIPS 140-1 Security Policy
Document Revision No.:	2.0.
Author:	Baltimore
Approved By:	Paul Goffin
Number of pages:	16
Revision Date:	27 March 2001