BALTIMORE

Baltimore ACCE SP

Security Policy 1447 SD0122

4.0

Table of Contents

1. Introduction

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

1.1. The Baltimore ACCE SP

The *Baltimore Advanced Configurable Crypto Environment – Security Processor (ACCE SP)* (see front cover picture) is a cryptographic module contained within a tamper resistant and detecting enclosure certified as meeting FIPS 140-1 level 4. It is similar to the *Baltimore Advanced Configurable Crypto Environment (ACCE)* (See FIPS PUB 140-1 certificate #112.) and shares many common components and features.

Like the ACCE, the ACCE SP is a *single user* module i.e.; it provides cryptographic services to exactly *one* user. This *single user* is an embedded firmware application which can only be generated and loaded by Baltimore or the module customer (this is ensured by FIPS approved cryptographic techniques (see Section 5: Identity Based Authentication for details). Note also that user code cannot be loaded dynamically, though authenticated field updates are possible.

The ACCE SP does 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.).

Both the ACCE & ACCE SP cryptographic module includes a commercial RISC (Reduced Instruction Set Computing) microprocessor which manages and/or undertakes the cryptographic services provided by the module. Dedicated hardware devices modules carrying out common cryptographic functions (modular exponentiation and symmetric algorithm operations) are also included.

1.2. The Europay NSP

The *Europay NSP* is an example of Baltimore product containing the ACCE SP combined with an application (the *single user* of the SP ACCE) to provide custom functionality (related to the on-line verification of credit-card Personal Identification Numbers (PINs)). The *Europay NSP* was developed for Europay (a major European financial institution) and utilises ACCE SP cryptographic functions such as Encrypt/Decrypt, Hash, MAC, Sign, Verify, Generate Keys, etc. to translate end-user PINs between data formats and encryption keys used by a number of other financial institutions (card issuers).

The Europay NSP physically consists of an ACCE SP 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 Europay NSP is designed to be connected to a private network which is connected to a number of member terminals and member data systems via “communication enpoints”, **not** to a public network. In operation, end-user PINs are accepted via the network, decrypted, reformatted and re-encrypted using DES or triple DES (FIPS PUB 46-3). Member financial institutions provide their own keys to NSPs via smart cards using split knowledge procedures.

The complete Functions Specification of the Europay NSP is contained in Baltimore document 1447-FS0055

2. Non-FIPS Operating Modes

2.1. General

The Baltimore ACCE SP offers a range of cryptographic facilities and mechanisms, subject to factory build options.

When operated in FIPS mode, the ACCE SP is certified to operate at FIPS 140-1 level 4 after the initialisation process is completed (Initialisation generates or imports the data used to authenticate Crypto Officers. It can also involve the import of application keys, subject to the design of the application. As an example, in the case of the Europay NSP, some application keys are imported during initialisation by firmware which is then erased and replaced with the eventual application. This process, which takes place in secure premises ensures that these keys cannot be subverted during eventual site operation.)

2.2. Support of non-FIPS algorithms

Non-FIPS modes of operation for cryptographic functions or non-FIPS approved algorithms 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*).

Non-FIPS modes of operation include the use of non-FIPS approved MACing methods, the potential use of RSA for encryption and custom functionality which converts data between various banking PIN formats. These modes are designed to support applications such as the Europay NSP.

2.3. Further non-FIPS operation

Unlike the ACCE, Crypto Officers cannot enable additional non-FIPS modes of operation.

3. Physical Security

3.1. Introduction

The ACCE SP is contained within an embedded module certified as meeting the requirements of FIPS 140-1 level 4.

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

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).

Once the IMK has been zeroised, on-site recovery (including any attempt to re-install firmware) of the ACCE is impossible. The unit 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 SP 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 Europay NSP) keys can be re-entered from member master media.

If the ACCE SP is further taken beyond its storage temperature range, it zeroises the IMK. (note the ACCE SP will have already halted, zeroised all user keys and the SMK). As stated above, once the IMK has been zeroised, on-site recovery is impossible.

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

The ACCE SP supports (single) User and Crypto Officer Roles.

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.
- Translate PIN format (non-FIPS mode)

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

There may be multiple Crypto Officers (Security Officers) who access the ACCE SP via the administration interface. This interface requires a display panel, keypad and SmartCard reader (as provided in the Europay NSP). The Crypto Officer cannot carry out user functions

Crypto Officers are identified via a challenge-response mechanism utilising a “shared secret” (non-FIPS derivation of DES keys from a single secret which is protected by the IMK).

Crypto Officers can:

- Import new (their own only) member keys (in component form).
- Change member (their own only) key attributes.

5. Identity Based Authentication

5.1. User

There is a single user of the ACCE SP Application Program Interface (API). This is the companion embedded application. This application is linked to the ACCE SP 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 the ACCE SP is restarted (i.e. power on) or reset, the MAC is recalculated and compared with the stored version. In the event that the ACCE SP 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 SP identifies and authenticates its 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 SP 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.

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)

- User Authentication:

  SSMK (Secure Software MACing 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 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.

    Keys can be encrypted either by the SMK (DES CBC) or via other *Transport keys* (Also DES CBC). Any user (encryption) key can be a transport key, but the application (for example the Europay NSP application) usually enforces a hierarchy.

  - 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 and IMK *never* leave the protected physical area.

7. Firmware Loading

7.1. Factory Firmware Download and Key Initialisation

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

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

Should an ACCE SP 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

The ACCE SP's application firmware 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 the ACCE SP, it will reject the download and restart using its existing firmware.

8. Maintenance

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

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

Configuration Control of this Document

Document details

File Name:	NSPSecurityPolicy-PublicVersion.doc
Document Title:	Baltimore ACCE SP - Security Policy 1447 SD0122
Document Revision No.:	4.0.
Author:	Baltimore
Approved By:	Paul Goffin
Number of pages:	15
Revision Date:	10 October 2000