**Ascom Hasler Mailing Systems**

# FIPS 140-1
# **Cryptographic Module Security Policy**
# for the
# Ascom Hasler Mailing Systems, Inc.
# SAFE™ CV Lite

Ascom Hasler Mailing Systems
19 Forest Pky.
Shelton, CT 06484

| | |
|---|---|
| Date: | 20-June-2001 |
| Version: | 1.4 |
| Short-Title: | SAFE CV Lite Crypto-vault Security Policy [Phase I] |
| Marking: | None |
| Provider: | Ascom Hasler Mailing Systems, Inc |
| Project-ID: | SAFE CV Lite |
| File-ID: | SAFE CV Lite Security Policy-1 v1.4 |

# Change History

| Version | Changes |
|---|---|
| 1.0 | Initial release of Security Policy for Phase I PSD. |
| 1.1 | Non-proprietary version of Security Policy for Phase I PSD. |
| 1.2 | Non-proprietary version of Security Policy for Phase I SAFE Crypto-vault. |
| 1.3 | CygnaCom revision to include the SAFE command set list and TDES PIN keys. |
| 1.4 | Change module name to SAFE CV Lite |

# Table of Contents

# Figures



# Tables

# 1 Introduction

## 1.1 Purpose

This is a Cryptographic Module Security Policy for the **ASCOM Secure Authentication Funds Engine (SAFE) Crypto-vault (CV) Lite**. This policy was prepared for the purpose of a FIPS 140-1 [FIPS94] certification of the SAFE CV Lite. FIPS 140-1 gives U.S. Government requirements for cryptographic modules, and defines the Security Policy as:

> *"A precise specification of the security rules under which the cryptographic module must operate, including rules derived from the security requirements of this standard, and the additional security rules imposed by the manufacturer."*

The security of the SAFE CV Lite Crypto-vault meets FIPS 140-1 level 3 requirements with respect to physical security (as specified in Section 4.5 in FIPS 140-1) and at least level 2 in all other aspects. As per USPS requirements, the module meets FIPS 140-1 Level 4 requirements for environmental failure testing (EFT).

This security policy describes how this is done and how the SAFE CV Lite Crypto-vault is to be used and operated in a secure fashion.

## 1.2 For more information

For more information about the FIPS-140-1 standard and validation program please visit the NIST web site at **http://csrc.nist.gov/cryptval**.

## 1.3 Terminology

The SAFE CV Lite Crypto-vault will be denoted as "**SAFE CV Lite**" throughout this document.

The Term "**indicia**" is used throughout this document to denote the digital Information Based Indicia as specified by the US Postal Service. All services and functions of the SAFE CV Lite provided with respect to indicia (like indicia generation, funds management and related diagnostics) are called collectively "**indicia application**".

# 2 Product Description

## 2.1 The SAFE CV Lite

The SAFE CV Lite device is designed as a single electronic circuit board with a serial external port and a power supply as interfaces. The board is sealed in a hard opaque heat transferring potting compound to eliminate the possibility that tampering can occur without significant visual damage to the board or board components. No physical access of any kind (e.g. battery replacement) is possible.

The main processor executes a static application, which is not changed in the field. The primary objective of this application is to protect the **Postal funds** and to apply respective access rules. Various memory components and supporting processors (like cryptographic processors) are used.

## 2.2 Purpose of the SAFE CV Lite

The SAFE CV Lite supports the creation of authorized indicia, which shows evidence of postage payment. The indicia consists of a two-dimensional bar code and certain human readable information such as a provider ID, model number, serial number, date of mailing, amount of postage, mailer's location (city & state or ZIP Code) and rate category.

The SAFE CV Lite provides for the accurate accounting of postal funds. It holds the funds needed for the postage and produces on request of the USPS customer digitally signed data sets, each representing indicia. It is designed to adhere to applicable USPS regulations.

### 2.3 Use of the SAFE CV Lite

The SAFE CV Lite is integrated in or connected to some host system under the custody of the customer (like a PC). The customer may access the SAFE CV Lite and instruct it to generate indicia on his behalf by using some application software running on the host system. The indicia will be used by the host system to produce the actual printed indicia on mail pieces with suitable printers.

The host system also provides a communication link (e.g. using a modem) to certain external entities with administrative or application related privileged responsibilities. These entities are part of the background infrastructure provided by ASCOM.

The ASCOM Telemeter Setting (TMS) data center is responsible for the (remote) download of new postal funds, the upload of audit information and other application management related operations.

The ASCOM CA acts as administrator and may access the SAFE CV Lite in manufacturing to manage cryptographic elements.

ASCOM may perform diagnostics operations with a SAFE CV Lite when it is returned from the customer to ASCOM and eventually re-manufacture the device or scrap it.

The SAFE CV Lite does not regard the host system as a secure or otherwise trusted environment. The communication between the SAFE CV Lite and any of those privileged entities introduced before are therefore protected by cryptographic means. The SAFE CV Lite itself has a secure containment.

### 2.4 Life Cycle of the SAFE CV Lite

The SAFE CV Lite is manufactured and initialized at ASCOM facilities and later on delivered to customers for operational use in the field. The SAFE CV Lite returns for decommissioning or for failures reported by the customer to ASCOM. If necessary, ASCOM may recover any postal funds stored in the SAFE CV Lite and arrange for the crediting of the respective amount to the customer.

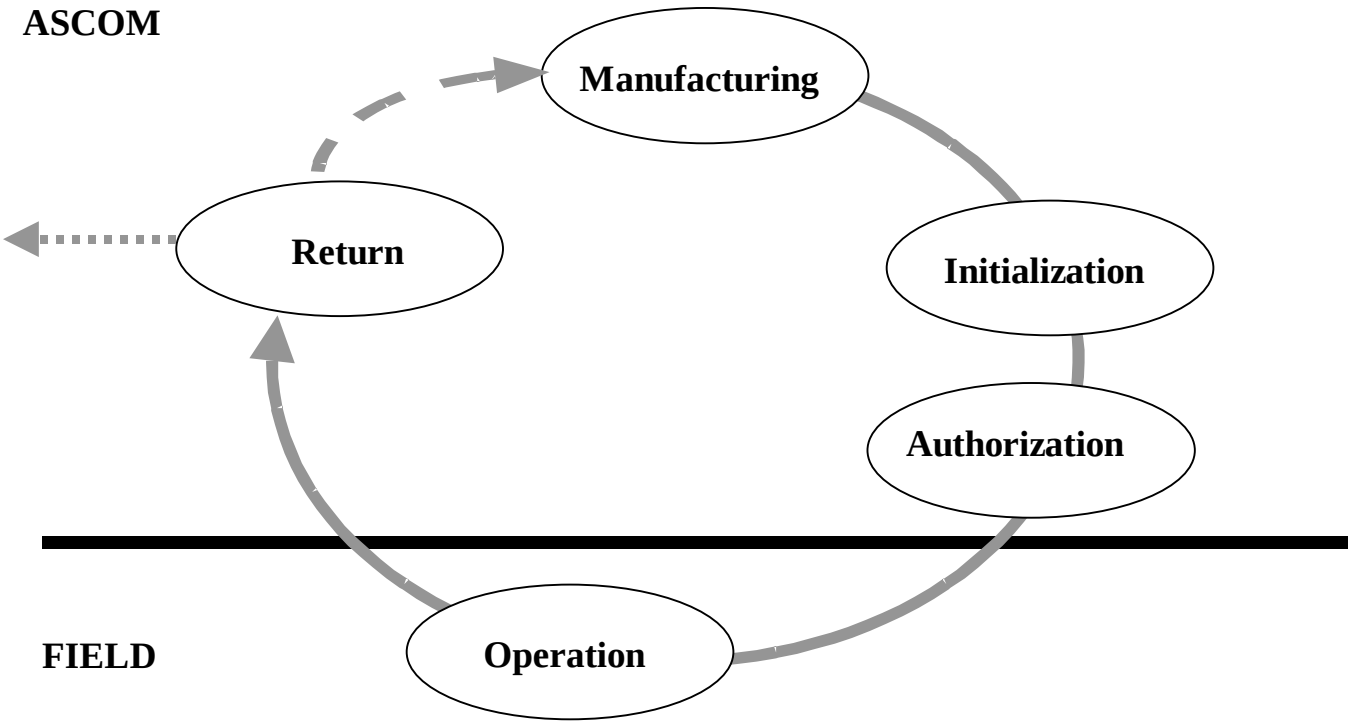


**Figure 1: Life Cycle of a SAFE CV Lite**

**Manufacturing** of the SAFE CV Lite is done in ASCOM facilities. The device is loaded with part of the cryptographic material and basic preparations for later use of the SAFE CV Lite are made. This includes

primarily the identification of the device and the initialization of its internal clock. Then, the SAFE CV Lite gets its enclosure making it ready for initialization.

**Initialization** makes the SAFE CV Lite ready for shipment into the field. This process, which also takes place on ASCOM premises, basically includes four steps:

1. Loading and initialization of the actual IBIP application software and related data.
2. Initialization of TMS key material used later on to secure the access of TMS to the postal funds (which itself will be loaded later on in the field).
3. Initialization of the Indicia Keys used to secure the digital Information Based Indicia later on in the field.
4. Initialization of the PIN keys used for secure transmission of the PIN for Customer authentication to the SAFE CV Lite.
5. Initialization of other cryptographic certificates used to authenticate administrative roles.

From now on until return to ASCOM (if given) the SAFE CV Lite is regarded as being in a potential hostile environment (the "field"). The SAFE CV Lite protects all assets including the postal funds, cryptographic material and available services according to the rules presented later on. Roles and Services are described subsequently.

An authorized dealer may ship the SAFE CV Lite to the customer as an alternative to direct shipment from ASCOM.

In the final steps of initialization a given SAFE CV Lite is **authorized** to a specific customer whose attributes are put into the SAFE CV Lite. Related (external) registration activities take place to make the SAFE CV Lite and the relationship to the given customer known to the background infrastructure (ASCOM and TMS). The SAFE CV Lite is now ready to be used by the customer from a technically point of view but has still no postal funds in it.

In the **Operation** phase it is the first step to load postal funds into the SAFE CV Lite, which is done by TMS. The customer may produce digital Information Based Indicia now using the available postal funds to his discretion. During the operational use TMS usually will communicate with the SAFE CV Lite from time to time in order to download new postal funds and to audit the device.

A Phase I SAFE CV Lite in the field may not undergo **Re-Keying**. During this phase, should the indicia key pair of a SAFE CV Lite need replacement, it is removed from service and replaced by a new one.

The SAFE CV Lite may be **Returned** for regular de-commissioning or other reasons (e.g. technical failure, suspected tampering) to ASCOM. ASCOM may access the SAFE CV Lite for diagnostic purpose and in order to recover the customer's postal funds stored in the SAFE CV Lite in a special return procedure. The SAFE CV Lite prevents any access to secret or private keys in that procedure. The SAFE CV Lite's internal hardware and connections are not replaceable. Any defect is unserviceable. Depending on the technical status of the device the SAFE CV Lite may be either destroyed or run again through manufacturing and initialization.

## 2.5 Security Objectives of the SAFE CV Lite

The SAFE CV Lite is primarily a secure device holding an amount of postal funds, which the USPS customer currently possessing the SAFE CV Lite may use to produce digital Information Based Indicia.

The following assertions apply to the SAFE CV Lite:

**A1 The major asset contained in the SAFE CV Lite is the current amount of postal funds stored in it.**

**A2 The customer may request the SAFE CV Lite to create digital Information Based Indicia.**

**A3 The SAFE CV Lite enforces the proper reduction of the available amount of postal funds as part of producing digital Information Based Indicia.**

**A4 The downloading of new postal funds may be initiated by the customer but not influenced otherwise. The downloading is done by TMS [1].**

**A5 The customer may recognize the status of the postal funds and the SAFE CV Lite in general.**

**A6 Any cryptographic data (e.g. keys, certificates and relevant cryptographic parameters) is initialized on ASCOM premises in a secure environment controlled by ASCOM Manufacturing [2].**

**A7 Any cryptographic data and the PIN can be zeroized by an operator callable command.**

**A8 Phase I SAFE CV Lite Cryptographic keys or certificates may not be changed in the field**

**A9 The modification of the SAFE CV Lite's software and its SW configuration is allowed to ASCOM Manufacturing only as part of the return procedure on ASCOM premises.**

**A10 Secret and private keys needed to enforce these security objectives never leave the SAFE CV Lite.**

These security objectives are fulfilled by the SAFE CV Lite by authenticating the respective roles and using the caller's role as reference for controlling the use of services and access to assets. This is done each time a service is requested from the SAFE CV Lite.

### 2.6 Physical Security

The physical Security of the SAFE CV Lite is governed by the physical security requirements of FIPS PUB 140-1 level 3. The security boundary of the SAFE CV Lite is encapsulated within a plastic enclosure filled with hard opaque potting material. There is no access to the internal components of the SAFE CV Lite without showing tamper evidence. The potting material offers a high degree of tamper resistance, causing physical destruction to components if removal is attempted. The SAFE CV Lite also utilizes tamper detection countermeasures that respond to tampering by zeroizing encryption keys and disabling the SAFE CV Lite from further use.

# 3 Roles, Services and Access Control

### 3.1 Roles and Authentication

Certain roles are identified by the SAFE CV Lite for the purpose of allowing access to services:

- ASCOM CA,
- ASCOM Manufacturing,
- TMS
- Customer.

ASCOM CA may access the SAFE CV Lite in manufacturing for the purpose of the management of cryptographic elements in the SAFE CV Lite and thus represent the "**Crypto Officer**" role during the key signature segment of the SAFE CV Lite.

ASCOM Manufacturing does bear the responsibility for initializing the SAFE CV Lite with cryptographic keying material during the Manufacturing and Initialization segment. ASCOM Manufacturing hence represents the

[1] The role "TMS" will be introduced in Section 3.1.
[2] The role "Ascom Manufacturing" will be introduced in Section 3.1.

"**Crypto Officer**" role on ASCOM's premises. ASCOM Manufacturing may never access the SAFE CV Lite in the field [3].

TMS and Customer represent the "**User**" role for the SAFE CV Lite, specifically the user of the indicia application.

Some services with an informative purpose only are provided by the SAFE CV Lite in the field and may be requested by anybody at any time. The external entity calling these services is not expected to take a certain role.

### 3.1.1 ASCOM CA

**ASCOM CA** represents the highest cryptographic authority of the key management system run by ASCOM for the indicia application. ASCOM CA enables the access of ASCOM Manufacturing to the SAFE CV Lite in the factory by issuing a public key certificate to ASCOM manufacturing. The self-certificate of ASCOM CA is stored in the SAFE CV Lite.

### 3.1.2 ASCOM Manufacturing

**ASCOM Manufacturing** represents the manufacturer of the SAFE CV Lite and is responsible for all SAFE CV Lite related activities on ASCOM's premises (manufacturing, initialization and return procedures).

### 3.1.3 TMS

**TMS** is responsible for controlling the postal funds in the SAFE CV Lite. TMS may only download new postal funds and activate or deactivate the indicia creation service. This is supported by an automatic watchdog mechanism in the SAFE CV Lite enforcing a periodical audit of the SAFE CV Lite's funds related services by TMS.

Cryptographic means are used as part of a specific protocol (TMS II protocol) to authenticate the respective sender of messages (TMS or the SAFE CV Lite). Data integrity and (if needed) confidentiality of messages are provided by the protocol as well.

The cryptographic security of the TMS II protocol is based on the following features:

- prevention of message replaying by the use of session keys and time variant parameters,
- mutual authentication of both the SAFE CV Lite and TMS,
- transaction data integrity using a MAC for each message,
- selective confidentiality for parts of the message as appropriate.

### 3.1.4 Customer

The **Customer** is allowed to use the SAFE CV Lite to produce indicia, which consumes the available postal funds in the SAFE CV Lite. In order to do so he has to perform a "login" into the SAFE CV Lite by presenting a PIN (for details see Section 3.3.8).

Moreover, the presence of the Customer is required to initiate the communication with TMS for funds related activities (like funds download).

## 3.2 Protected Assets

The major asset hold in the SAFE CV Lite is the currently available amount of postal funds. Some more objects are identified in order provide a more detailed picture of the SAFE CV Lite's access control policy.

[3] Note, that this is organizational assumption. This has to be ensured by ASCOM.

**Table 1: Protected Objects**

| |
|---|
| SAFE CV Lite configuration |
| Indicia application configuration |
| Postal Funds |
| Customer Attributes |
| Statistics and Records |
| Cryptographic keying material |

### 3.2.1 SAFE CV Lite configuration

Hardware and software of the SAFE CV Lite are configured in the manufacturing and initialization phase on ASCOM's premises. The **SAFE CV Lite configuration** is the hardware and software along with more basic operational parameters and data objects of the SAFE CV Lite in the field [4]. Operational parameters and data objects included for example date and time (along with related parameters) and any data identifying the hardware and software (e.g. meter serial number).

Any modification of the hardware or software of a SAFE CV Lite having been in the field requires the return of the device to ASCOM facilities beforehand, following proper return procedures (see Section 2.4).

### 3.2.2 Indicia application configuration

Various parameters, some of them being defined specifically for a customer, are used to control the indicia application. These parameters include various limits applied when performing indicia related transactions.

### 3.2.3 Postal Funds

The most important data item managed by the indicia application is the amount of **postal funds,** which is available for consumption via indicia generation. Specific security requirements imposed by USPS apply to the postal funds related management functions and access methods. Basically the postal funds are decreased every time an indicium is generated and increased by a TMS originated download of new funds.

### 3.2.4 Customer Attributes

Various attributes are used to identify and describe a specific customer. These **customer attributes** include a license ID, a corresponding ZIP code and the Customer's accounting number used by TMS for accounting purposes.

### 3.2.5 Statistics and Records

The SAFE CV Lite maintains various **statistics and records** about the use of services related to the postal funds and indicia generation. These statistics and records include recent transactions and various events like reaching application related limits, funds transfers from TMS, errors, warnings and the modification of parameters related to those services.

### 3.2.6 Cryptographic keying material

A digital signature generated with a dedicated private key stored in the SAFE CV Lite primarily secures the indicia. Other cryptographic keys are used to authenticate the roles ASCOM CA, and ASCOM Manufacturing. Domain parameters used by any cryptographic mechanisms are also regarded as being a part of the **cryptographic keying material**.

Keys and certificates stored in a SAFE CV Lite consist of:

[4] It is this configuration, which is primarily subject to security policy considerations in this document!

- the public key certificate of ASCOM CA,
- the public key certificate of ASCOM Manufacturing,
- the private indicia keys used to sign the indicia generated by the SAFE CV Lite,
- the public key certificate for the indicia keys,
- the public/private key pair used for secure download of the TMS keys,
- the secret symmetric TMS keys used to authenticate the access to the SAFE CV Lite by TMS, and
- the secret symmetric PIN keys used to decrypt the securely transmitted PIN received from the Customer.

The meaning and use of the cryptographic keying material is described in more detail in Section 3.3.7 and Section 4.

## 3.3 Services and Access Control Policy

The SAFE CV Lite provides various services to external entities as presented in Table 2 and described hereafter.

**Note.** This security policy focuses on the SAFE CV Lite in the field and to the Return phase (See sect. 2.4). References to manufacturing related phases (Manufacturing and Initialization) are made here only to provide the reader with a complete picture of the overall life cycle.

**Table 2 : SAFE CV Lite Services**

| Service | Access allowed for | Life cycle phase |
|---|---|---|
| General SAFE CV Lite Initialization | ASCOM Manufacturing | Initialization |
| Customer Specific Initialization | ASCOM Manufacturing | Authorization |
| Funds Download | TMS | Operation |
| Indicia Generation | Customer | Operation |
| Log Extraction | TMS<br>ASCOM Manufacturing | Operation<br>Return |
| Information | All | Operation / Return |
| Management of Cryptographic Services | ASCOM Manufacturing | Initialization / Return |
| Customer Authentication | Customer | Operation |
| Enabling/Disabling SAFE CV Lite | TMS | Operation |

### 3.3.1 General Device Initialization

ASCOM Manufacturing will initialize the SAFE CV Lite device when it leaves the Manufacturing phase. This process will initialize the indicia application along with all its related data completely as defined by ASCOM Manufacturing. The new application is loaded into the SAFE CV Lite as part of the functions related to this service.

Certain special diagnostic applications and other initialization applications are used by ASCOM Manufacturing in the initialization phase of the SAFE CV Lite in order to initialize various data objects and finally to load the indicia application itself taking over the control for use of the SAFE CV Lite in the field.

Data to be initialized includes the current date and time and attributes which identify and describe the specific device.

### 3.3.2 Customer Specific Initialization

This service includes functions performed by TMS in the field in order to configure the SAFE CV Lite for the use with a specific customer.

This includes loading of attributes identifying and describing the specific SAFE CV Lite in relation to the customer.

### 3.3.3 Funds Download

The indicia application services provide the most essential functionality of the SAFE CV Lite as these services cause the modification of the postal funds managed by the indicia application. All indicia are signed by the SAFE CV Lite using the indicia private key.

TMS may access the SAFE CV Lite in the field for downloading of new funds. Technically, this is done via the Host as intermediate system and using a specific protocol ("TMS II protocol").

TMS carries out the following operations as part of the TMS II protocol:

- receives a request for download of new funds and grants new funds after having performed suitable checks and
- performs a check of the value of postal funds in the SAFE CV Lite allowing TMS to compare it with available information for correctness ("device audit"),
- reads various values and parameters of the SAFE CV Lite configuration, the Indicia application configuration and the customer attributes,
- may modify the SAFE CV Lite's date-and-time,
- releases the SAFE CV Lite for further use.

The SAFE CV Lite tracks the remaining amount of available funds and the total amount of funds used for indicia creation with the given SAFE CV Lite so far [5].

A SAFE CV Lite internal Watchdog timer is used to automatically inhibit further indicia creations until proper device audit is done by TMS. The timeout can be configured and is typically a month.

### 3.3.4 Indicia Generation

The customer may generate indicia using the available funds. The creation of indicia decreases the available amount of funds while it increases the overall sum of funds used. Any other change of the funds is restricted to TMS.

A precondition for indicia generation is that the SAFE CV Lite indicia application function is not disabled because of an overdue audit (see above).

### 3.3.5 Log Extraction

ASCOM TMS may extract statistics for diagnostic and audit purposes either in the field or as part of the Return procedures.

### 3.3.6 Information

The SAFE CV Lite provides service functions to access various information available in the SAFE CV Lite. This information is generally not regarded as confidential. The respective service commands may be accessed therefore without the need of a preceding authentication.

[5] These values are referred to conceptually as "descending register" and "ascending register", see [USPS].

Information available includes:

- the current amount of postal funds,
- the value of various application relevant parameters (like applicable limits),
- various attributes identifying and describing the specific customer and the device,
- diagnostics and status information about the SAFE CV Lite device

### 3.3.7 Management of Cryptographic Services

ASCOM Manufacturing may query and set various elements of the SAFE CV Lite's cryptographic material (see Section 3.2.6) within the context of the key management concept described in Section 4.

Available functions for ASCOM Manufacturing in the initialization phase are

- Initiate the generation of indicia key pairs in the SAFE CV Lite and get the public key component from the SAFE CV Lite in the initialization phase,
- Initiate the generation of the TMS keys' El Gamal key pair to establish a shared symmetric key and extraction of the public key component from the SAFE CV Lite,
- Initiate the generation of the PIN keys used to decrypt the securely transmitted PIN received for Customer authentication to the SAFE CV Lite,
- Set and verify cryptographic parameters used for indicia generation.

### 3.3.8 Customer Authentication

The Customer is authenticated using a PIN based mechanism. The PIN is set to a random initial value in the Initialization phase. This value is made known to the customer using a communication path being different to the shipping of the SAFE CV Lite itself.

The SAFE CV Lite expects the PIN to be entered each time after powering up. The SAFE CV Lite also expects the PIN authentication procedure to be performed again each time the synchronization at the serial interface between the SAFE CV Lite and the host system gets lost. This event indicates to the SAFE CV Lite that it might have been moved to a different host system.

PIN authentication must be performed before any indicia application function is allowed by the SAFE CV Lite (indicia generation and TMS activities).

Whenever a specific consecutive number of authentication failures have occurred the PIN authentication function is locked, which effectively prevents the access to the indicia generation.

At the first power-up of an initialized SAFE CV Lite, the Customer enters the PIN through a keypad on the host/base. The host/base remembers this initial PIN by storing it in non-volatile memory. During subsequent power-ups, the host/base transmits the stored PIN, via key exchange with the SAFE CV Lite, which then encrypts the PIN and transfers it to the SAFE CV Lite. The Customer is not forced to re-enter the PIN at each power-up since this is the only role that accesses the module through this interface in the field.

### 3.3.9 Enabling/Disabling the Device

Based on several pre-defined security criteria (e.g. time, postal funds or piece count based limits), operations of a SAFE CV Lite in the field may be enabled/disabled remotely by TMS in case one or more of the criteria are met.

### 3.3.10 Service Command Set

GET_ACCOUNT_NUMBER

SET ACCOUNT NUMBER

GET_ACCOUNTING_REGISTERS

LOAD APPLICATION
START APPLICATION
WRITE APPLICATION BLOCK
GET_APPLICATION_IDENTIFIER
GET_APPLICATION_VERSION
GET ASCOM CERTIFICATE
SET ASCOM CERTIFICATE
GET ASCOM CERTIFICATE BOOT
SET ASCOM CERTIFICATE BOOT
GET_BATTERY_EXPIRATION_DATE
SET_BATTERY_EXPIRATION_DATE
COPY BOOT LOADER
WRITE BOOT LOADER BLOCK
GET BOOT LOADER FCS
INITIALIZE CRYPTOPROCESSORS
GET_CUSTOMER_INFORMATION
SET_CUSTOMER_INFORMATION
GET_CUSTOMER_TYPE
GET_DATE_TIME_LOCAL
GET_DATE_TIME_UNIVERSAL
SET_DATE_TIME_UNIVERSAL
GET_DAYLIGHT_SAVINGS
SET_DAYLIGHT_SAVINGS
PERFORM_DIAGNOSTICS
GET_DIGITS_AFTER_POINT
SET_DIGITS_AFTER_POINT
GENERATE ENCRYPTION KEY PAIR
GET ENCRYPTION PUBLIC KEY
GET_HARDWARE_SERIAL_NUMBER
GET_HARDWARE_VERSION_NUMBER
SET_HARDWARE_VERSION_NUMBER
GENERATE_INDICIUM
GET INDICIA CERTIFICATE
SET INDICIA CERTIFICATE
GET INDICIA COMMON PARAMETERS
SET INDICIA COMMON PARAMETERS
GENERATE INDICIA KEY PAIR
GET INDICIA PUBLIC KEY

GET_INTERFACE_STATUS

KMS_MESSAGE

GET_DEVICE_ID

SET_DEVICE_ID

GET_LICENSING_ZIP_CODE

SET_LICENSING_ZIP_CODE

GET_LIMITS

SET_LIMITS

START_LOADER

GET LOADER VERSION

GET_LOCAL_TIME_OFFSET

SET_LOCAL_TIME_OFFSET

GET LOG

PERFORM LOG TEST

LOGIN

LOGOUT

GET_MANUFACTURE_DATE

SET_MANUFACTURE_DATE

START_MANUFACTURING ROLE

READ MEMORY BLOCK

WRITE MEMORY BLOCK

CHANGE_PIN

RESET PIN

START_PIN

GET_POST_DATE_TIME_LIMIT

SET_POST_DATE_TIME_LIMIT

START_SELF-TEST

INITIALIZE PSD

GET_PSD_OWNER

SET_PSD_OWNER

GENERATE_QUICK_INDICIUM

GET_QUICK_INDICIUM

GET_REMAINING_POSTAGE_VALUE_REFUND

VERIFY_ROOT_SIGNATURE

GET_STATE

SET_STATE

TMSII_PROTOCOL_START

TMSII_PROTOCOL

SET TMS KEY TRIPLE

SET TMS PUBLIC KEY

GET_WATCHDOG_CONFIGURATION

SET_WATCHDOG_CONFIGURATION

# 4 Key Management

The following cryptographic elements are permanently stored in the SAFE CV Lite:

- ASCOM CA certificate,
- ASCOM Manufacturing certificate,
- Indicia key pair,
- Indicia public key certificate,
- PIN keys,
- TMS key pair, and
- TMS keys.

Table 3 provides an overview of these cryptographic elements, which will be explained afterwards.

**Table 3 : Cryptographic elements permanently stored in the SAFE CV Lite**

| Cryptographic element (Key or certificate): | Generation | Initialization | Usage | Replacement | Destruction [6] |
|---|---|---|---|---|---|
| ASCOM CA certificate | Issued by ASCOM CA | Initialization phase | **Authentication** of ASCOM CA<br>**Verify** ASCOM Manufacturing certificate | SAFE CV Lite replacement | When replaced |
| ASCOM Manufacturing certificate | Issued by ASCOM CA | Initialization phase | **Authentication** of ASCOM Manufacturing | SAFE CV Lite replacement | When replaced |
| Indicia key pair | Generated by SAFE CV Lite | Initialization phase | **Indicia generation** in the field<br>**Signing** of message exchanges with ASCOM infrastructure | SAFE CV Lite replacement | When return application is loaded |
| Indicia public key certificate | Issued by USPS Infrastructure | Initialization phase | **Verify** printed indicia | SAFE CV Lite replacement | When return application is loaded |
| PIN keys | Generated by SAFE CV Lite | Initialization phase | **Decrypt** securely transmitted PIN received for Customer authentication | SAFE CV Lite replacement | When return application is loaded |
| TMS key pair | Generated by SAFE CV Lite | Initialization phase | **Secure** download of TMS keys to the SAFE CV Lite | SAFE CV Lite replacement | When return application is loaded |
| TMS keys | Generated by SAFE CV Lite and TMS | Initialization phase | **Authentication** of TMS<br>Data **integrity** and **confidentiality** | None [7] | When return application is loaded |

### 4.1 ASCOM CA certificate

The **ASCOM CA certificate** is a self-certificate issued by the ASCOM CA using a DSA public/private key pair. It is used by the SAFE CV Lite to verify the ASCOM Manufacturing certificate.

The ASCOM CA certificate is stored into the SAFE CV Lite as part of the Initialization phase.

### 4.2 ASCOM Manufacturing certificate

The **ASCOM Manufacturing certificate** is issued and verified by the ASCOM CA using a DSA public/private key pair. It is used by the SAFE CV Lite to authenticate the ASCOM Manufacturing role.

[6] If a SAFE CV Lite is deemed as not reusable in the return phase, it will be virtually destroyed. This implies in particular to the destruction of all sensitive information, such as certificates and cryptographic keys, in the SAFE CV Lite. The SAFE CV Lite serial number is physically destroyed and recorded as such through the administrative processes.

[7] Actual TMS session keys get modified in a non-predictable way as part of the next TMS-II protocol run.

The ASCOM Manufacturing certificate is stored into the SAFE CV Lite as part of the Initialization phase.

### 4.3 Indicia key pair

The **Indicia DSA key pair** is generated by the SAFE CV Lite itself. This process is initially performed in the initialization phase. The public key is extracted by ASCOM Manufacturing and transferred to USPS IBIP key management infrastructure for certification.

Later on in the field should the Phase I SAFE CV Lite require a replacement of the Indicia key pair (re-keying), it will result in supplying a replacement SAFE CV Lite.

### 4.4 Indicia public key certificate

The **Indicia public key certificate** is issued by the USPS IBIP key management infrastructure. The certificate is issued after the indicia public key has been received from ASCOM Manufacturing. The certificate is used to verify the SAFE CV Lite's printed indicia. This process is performed in the initialization phase.

### 4.5 PIN keys

**PIN keys** are Triple DES symmetric keys generated by the SAFE CV Lite and used for secure transmission of the Customer PIN. This process is initially performed in the initialization phase.

The encrypted PIN is transmitted by the host/base and then decrypted by the SAFE CV Lite to authenticate the Customer.

### 4.6 TMS keys

**TMS keys** are Triple DES symmetric session keys used solely by TMS to communicate securely with the SAFE CV Lite using a special protocol to ensure data authenticity, integrity and confidentiality.

ASCOM Manufacturing commands the SAFE CV Lite in the Initialization phase to generate a special public/private key pair, where the underlying public key crypto system (ElGamal) allows for the establishment of a shared secret key. ASCOM Manufacturing transfers this public key to TMS, which uses the key to establish the shared secret for download of the initial TMS keys (three symmetric keys) securely to the SAFE CV Lite. Thus, only TMS and the SAFE CV Lite know the TMS keys. The ElGamal public/private key pair will not be used for any other purpose.

(Initial) TMS keys are modified the first time they are used as part of the TMS II protocol (see Section 3.1.3). The modification is done synchronously by both TMS and the SAFE CV Lite as part of the TMS II protocol mechanisms. There is no complete replacement of the TMS keys in the field like initiating a new key sequence. As the systematic key modification is a built-in feature of the TMS-II protocol, no separate crypto officer role is needed.

# 5 Annex

### 5.1 References

[FIPS94] Federal Information Processing Standards Publication 140-1: Security Requirements for Cryptographic Module, 1994.

[USPS] United States Postal Service (USPS): Information-Based Indicia Program (IBIP): Performance criteria for information-based indicia and security architecture for open IBI postage evidencing systems (PCIBI-O). February 23, 2000 – Draft

### 5.2 Acronyms

DES Data Encryption Standard

| | |
|---|---|
| DSA | Digital Signature Algorithm |
| FIPS PUB | Federal Information Processing Standard Publication |
| IBI | Information Based Indicia |
| IBIP | Indicia Based Information Program |
| PIN | Personal Identification Number |
| TMS | TeleMeter Setting System |