Ascom Hasler Mailing Systems, Inc.
19 Forest Parkway
Shelton, CT 06484

ascom

FIPS 140-1

Cryptographic Module Security Policy

for the

Ascom Hasler Mailing Systems, Inc.
Production Postal Security Device
SAFE CV 401

Date:	29 October 2001
Version:	383SYS002B ver.6.4
File:	PSD Security Policy 64.doc

Approvals

Organization	**Responsibility**	**Date**
Engineering	Name: Signature:	
Project Management	Name: Signature:	
	Name: Signature:	
	Name: Signature:	

Change History

Version	By	Changes
0.1	L. Frey	First Edition
0.2	L. Frey	The open questions have been transferred to a new document dedicated to that.
1.0	L. Frey	First distributed version.
1.1	L. Frey	Revision based on the answers to open questions (s. [s3lab3], [ASC3]) and new revision 1.3 of the SBB Specification.
1.2/1.3/1.4		Internal Review
2.0	L. Frey	Release S^3lab, distributed to Ascom Hasler
2.1	L. Frey	Internal Review: major modifications are: • Use of input from 1) "Software Requirements Specification Postal Security Device" 2) "IBIP Interim Submission Concept of Operations" 3) "PSD Baseline Requirements & Architecture" • Slight restructuring of the document using an example certificate (DS 1954 Cryptographic iButton) as background to make the security policy more "marketing oriented" and "management readable" • New section 4 to describe key management issues more coherent. • No editor's notes in the document any more. A separate document ("Underlying assumptions" provided by S^3lab) summarizes any assumptions or open questions. • The role/object/services concept is made more taut in order to emphasize more plain what is the essence of the security policy, i.e. less objects and services and more generalized items.
2.2		Internal Review
3.0	L. Frey	Release S^3lab, distributed to Ascom Hasler
3.1/3.2	L. Frey	Reviews, adjustment to key management concept release 0.9/DRAFT, Release to Meeting in Shelton 10.3.99-12.3.99
4.0/4.1	L. Frey	Changes due to the results of the meeting 11.3.99 in Shelton.
5.0	L. Frey	Major revisions, reflecting the important changes of the USPS IBIP specifications and the resulting modifications of the ASCOM key management system.
6.0	G. Brookner	Major revision. Updated to reflect Remote Control capability of the production PSD in the field as well as the certificate hierarchy. Updated to reflect the Diffie-Hellman authenticated KMS session.
6.2	L. Frey	Updated to include new worldwide key hierarchy structure and storage of certificates in PSDs.
6.3	G. Brookner M Ferraro	Clarified key zeroization, removed confidential footer, misc. spelling errors. Updated in response to Cygnacom's comments (07.July.2001).
6.4	R. Saunders	Sections 1.1 para 4; 2.4 initialization, authorization, operation; and 4 updated in compliance with NIST recommendations.

Table of Contents

Figures

Tables

1 Introduction

1.1 Purpose

This is a Cryptographic Module Security Policy for the **ASCOM Postal Security Device**. This policy was prepared for the purpose of a FIPS 140-1 [FIPS94] certification of the Postal Security Device. 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 Postal Security Device meets FIPS 140-1 level 3 requirements with respect to physical security (as specified in section 4.5 in FIPS 140-1) and level 3 in all other aspects. Per USPS requirements, the module meets FIPS 140-1 Level 4, Environmental Failure Testing (EFT).

This security policy describes how this is done and how the Postal Security Device is to be used and operated in a secure fashion. The module operates only in a FIPS compliant mode and does not support a non-FIPS mode.

1.2 Terminology

Ascom's Secure Funds Authenticated Funds Engine (SAFE), model SAFE CV 401/411, will be denoted as "**PSD**" 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 PSD provided with respect to indicia (like indicia generation, funds management and related diagnostics) are called collectively "**indicia application**".

The acronym "**TMS**" (for "TeleMeter Setting System") is used to denote a certain PSD external entity entitled to perform privileged operations on the indicia application (like downloading of funds).

The acronym "**KMS**" (for "Key Management System") is used to denote a certain PSD external entity entitled to perform privileged operations related to the management of cryptographic material.

2 Product Description

2.1 The Postal Security Device (PSD)

The PSD device is a multiple chip embedded module designed as a single electronic circuit board with interfaces to a serial external port and a power supply. The board is enclosed with a tamper detecting "continuity" mesh and sealed in a hard opaque heat transferring potting compound. Together these elements both conceal the electronic circuitry and provide for tamper detection and response. Further, tampering cannot occur without significant visual

damage to the potting material, board or board components. No physical access to the PSD (e.g. battery replacement) is possible.

The main processor executes a static application. 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.

The general architecture of the PSD is depicted in the following diagram. The difference between the SAFE CV 401 and SAFE CV 411 is the external enclosure form factor.

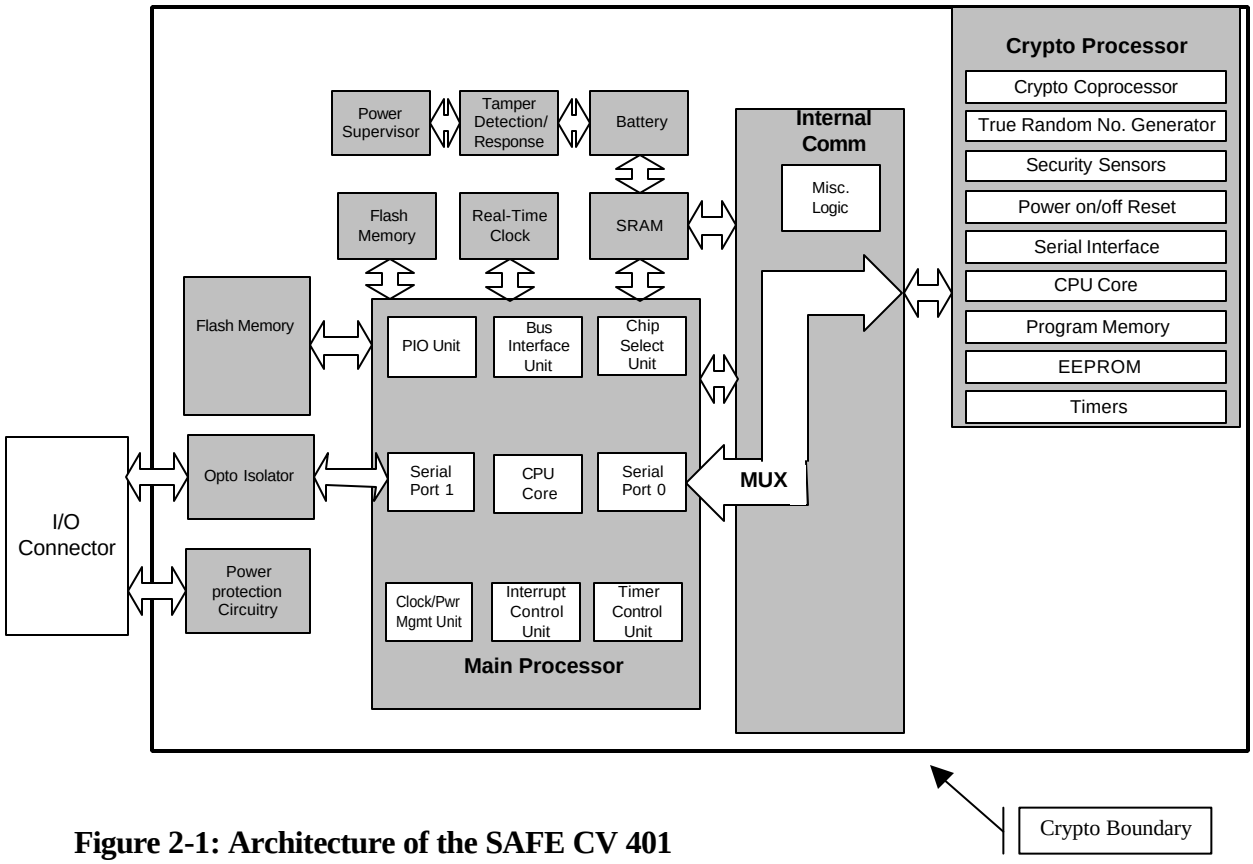

Figure 2-1: Architecture of the SAFE CV 401

2.2 Purpose of the Postal Security Device (PSD)

The PSD 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 Device ID Number, date of mailing, amount of postage, mailer's location (city & state or ZIP Code) and rate category.

The PSD 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 [USPS00].

2.3 Use of the Postal Security Device (PSD)

The PSD is integrated in or connected to some host system under the custody of the customer (like a PC or within a metering/mailing device). The customer may access the PSD 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.

ASCOM Regional CA and ASCOM Remote Control acting as administrators may access the PSD in the field (remotely) and are allowed to manage cryptographic elements.

ASCOM may perform diagnostic operations with a PSD when it is returned from the customer to ASCOM, thereafter leading to the PSD being re-manufactured or scrapped.

The communication between the PSD and any of those privileged entities introduced before are protected by cryptographic means. The PSD itself has a secure containment.

The entity “KMS” or more precisely its logical constituents ASCOM Regional CA, ASCOM Remote Control and TMS may access the PSD in the field (remotely) and are allowed to provide such operations as changing cryptographic keys, disabling PSDs, providing secure session operations for the exchange of protected data with the PSD. These processes provide authentication, integrity protection and encryption means for said data interchanges.

2.4 Life Cycle/Phases

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

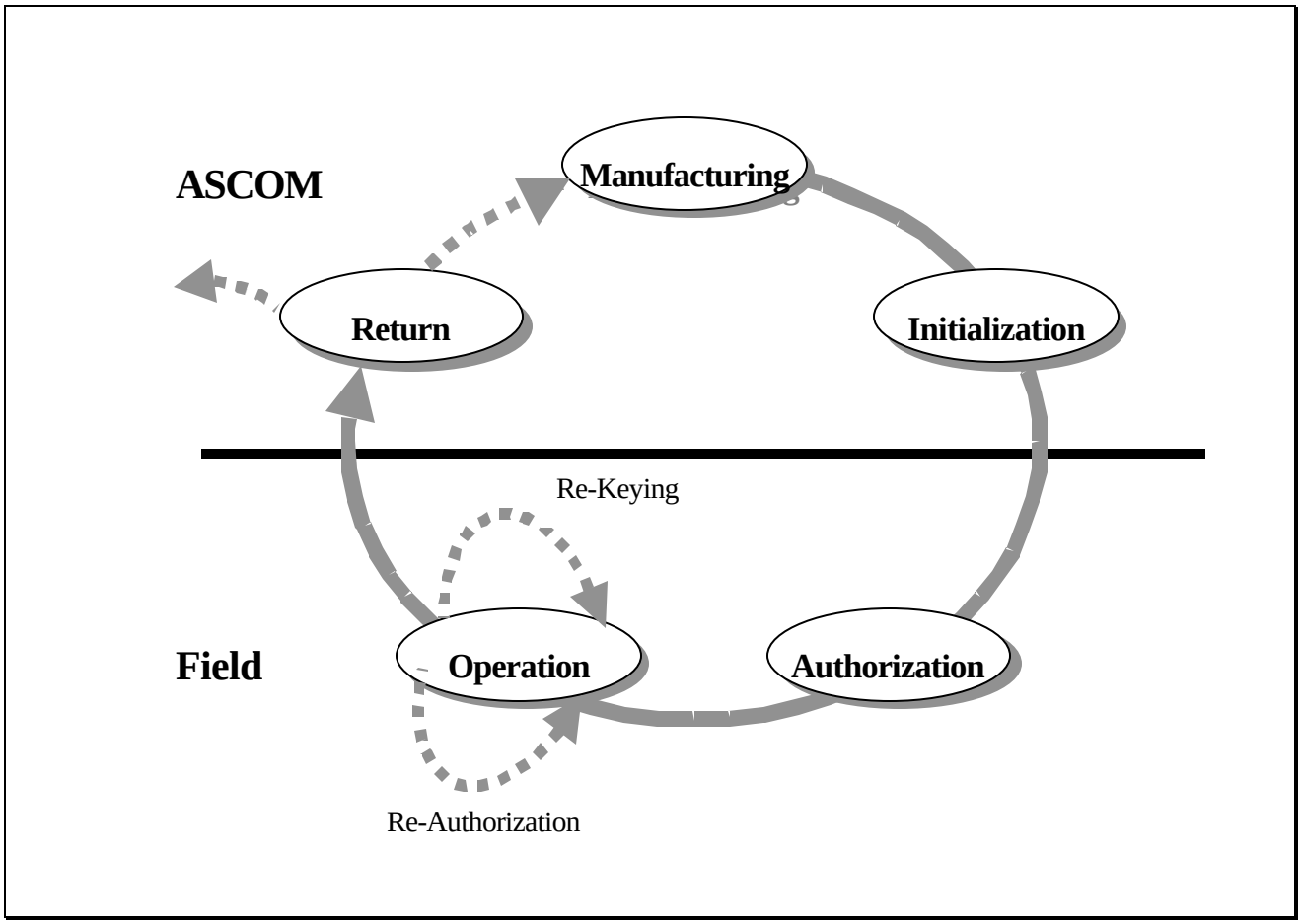

Figure 2-2: Principle Life Cycle of the PSD

Manufacturing of the PSD is done in ASCOM facilities and consists of basic preparations of the PSD for its later use. This includes primarily the identification of the PCB and the initialization of the PCB's internal clock. Then, the enclosure is put on the PCB making the PSD ready for initialization.

Initialization makes the PSD ready for shipment into the field. This process, which also takes place on ASCOM premises, basically includes the following steps:

1. Loading and initialization of the actual IBIP application software and related data.
2. Initialization of PSD Authentication Keys used to establish a secure communication later on between a PSD in the field and the ASCOM infrastructure.
3. Initialization of the PIN keys used for secure transmission of the PIN for Customer authentication to the PSD.
4. Loading of cryptographic certificates used to authenticate administrative roles.

From now on and until returned to ASCOM, the PSD is considered as being in a potential hostile environment (the "field"). The PSD protects all assets including the postal funds, cryptographic material and available services according to the rules presented herein. Roles and Services are described subsequently.

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

In the **Authorization** phase, a given PSD is assigned to a specific customer whose attributes are put into the PSD. Related (external) registration activities take place to make the PSD and the relationship to the given customer known to the background infrastructure (ASCOM and TMS). The PSD is now ready to be used by the customer from a technical point of view, but has still no postal funds in it.

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

A PSD in the field may run through a new, partial Authorization (referred to as **Re-Authorization**), remotely controlled by ASCOM, if arises (e.g. due to changed customer data as address).

A PSD in the field may undergo **Re-Keying**, remotely controlled by ASCOM Remote Control. During this phase all or part of the cryptographic keying material (private keys, public key certificates) stored by the PSD may be replaced by new one.

The PSD may be **returned** for regular de-commissioning or other reasons (e.g. technical failure, suspected tampering) to ASCOM. ASCOM may access the PSD for diagnostic purpose and in order to recover the customer's postal funds stored in the PSD. However, the PSD prevents any access to secret or private keys in that procedure. The SAFE's internal hardware and connections are not replaceable. Any defect is unserviceable. Depending upon the operational status of the PSD, it may either be destroyed or sent through the manufacturing and initialization process.

2.5 Security Objectives of the Postal Security Device (PSD)

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

The following assertions apply to the PSD:

A1 The major asset contained in the PSD is the current amount of postal funds stored in it.

A2 The customer may request the PSD to create digital Information Based Indicia.

A3 The PSD enforces the proper reduction of the available amount of postal funds as part of producing a 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.

A5 The customer may recognize the status of the postal funds and the PSD in general.

A6 Initial cryptographic data (e.g. keys, certificates and relevant cryptographic parameters) required for authentication is initialized on ASCOM premises in a secure environment controlled by ASCOM Manufacturing.

A7 Cryptographic keys or certificates may be changed in the field. This is an administrative responsibility of ASCOM KMS entities (e.g. ASCOM Regional CA and/or ASCOM Remote Control).

A8 Secret and private keys needed to enforce these security objectives never leave the PSD.

These security objectives are fulfilled by the PSD 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 PSD.

2.6 Physical Security

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

3 Roles, Services and Access Control

3.1 Roles and Authentication

Certain roles are identified by the PSD for the purpose of allowing access to services:

- ASCOM Root CA,
- ASCOM Regional CA,
- ASCOM Manufacturing,
- ASCOM Remote Control,
- TMS,
- Customer.

ASCOM Root CA is the highest level of authority in the certificate hierarchy and is the identity that assumes the Crypto Officer role that is enacted to issue all ASCOM Regional CA certificates used by the PSD to authenticate regional KMS entities. ASCOM Root CA also signs PSD-resident applications.

Both entities, ASCOM Regional CA and ASCOM Remote Control, may access the PSD in the field for the purpose of the management of cryptographic elements in the PSD and thus represent the "Crypto Officer" during the operational phase of the PSD.

ASCOM Manufacturing has the responsibility for initializing the PSD with cryptographic keying material during the manufacturing and initialization phase. ASCOM Manufacturing thus represents the "Crypto Officer" on ASCOM premises. ASCOM Manufacturing may never access a PSD in the field.

TMS and Customer represent the “User” of the PSD, specifically the user of the indicia application. Some services with an informative purpose only are provided by the PSD in the field and may be requested by an entity at any time (e.g. Licensing Zipcode, Account Number, Customer Type, Daylight Savings, Time Zone (Local Time), PSD Owner). The external entity calling these services is not expected to explicitly represent a certain role to the PSD.

3.1.1 ASCOM Root CA

ASCOM Root CA represents the highest cryptographic authority of the key management system run by ASCOM for the indicia application and as such issues all certificates of the next lower level of the KMS, i.e. the ASCOM Regional CA certificates.

The self-signed certificate of ASCOM Root CA is stored in each PSD.

3.1.2 ASCOM Regional CA

ASCOM Regional CA represents the highest cryptographic authority of a KMS for a single country or region of a country.

It acts as the Certification Authority for its population of PSDs and the other regional KMS entities.

ASCOM Hasler maintains control over the Region Change process. No Regional KMS can take over control of PSDs that belong to a different Regional KMS. All PSDs that are shipped from ASCOM Hasler Manufacturing are "generic" and can be assigned to any region. But any PSD assigned to a particular region can change its region only back to ASCOM Hasler Manufacturing.

3.1.2.1 Regional KMS

A regional KMS supports all PSDs within a single country or defined region of that country (excluding the ASCOM Factory Region). As the highest local cryptographic authority, the ASCOM Regional CA issues all Remote Control certificates and issues all PSD Authentication certificates in that particular region.

3.1.2.2 ASCOM Factory Region

The Factory Region is a dedicated regional KMS introduced to provide the cryptographic support for the manufacturing and initialization of new PSDs and the return of PSDs from the field. The structure of its KMS is identical to the one of any other regional KMS. Thus, the Factory Region has its own ASCOM Regional CA that signs all ASCOM Manufacturing certificates. It also issues the PSD Authentication certificate for a PSD under manufacture.

3.1.3 ASCOM Manufacturing

ASCOM Manufacturing represents the manufacturer of the PSD and is responsible for all activities applied to the PSD within the premises of ASCOM (manufacturing, initialization and return procedures). The Manufacturing entity exists only in the Factory Region, and authenticates the KMS to a PSD under manufacture, or after its return from a customer.

3.1.4 ASCOM Remote Control

ASCOM Remote Control directly or on behalf of ASCOM Regional CA, is authorized and responsible for accessing the PSD for various administrative purposes in the field. This includes:

- initiating the generation of a new indicia key pair (re-keying),
- resetting the customer's PIN,
- loading the customer specific data in the (Re)-Authorization phase,
- enabling or disabling the indicia application and
- extracting indicia application related statistic and logfiles [1].

Each message from ASCOM Remote Control is authenticated by the PSD. In particular, all messages exchanged for the purpose of replacing an indicia key pair are protected by cryptographic means. While digital signatures provide entity authentication and data integrity, data confidentiality is protected by symmetric encryption.

3.1.5 TMS

TMS is responsible for controlling the postal funds in the PSD. 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 PSD enforcing a periodical audit of the PSD'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 PSD) and to protect the data integrity and (if needed) confidentiality of the message exchanges.

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

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

3.1.6 Customer

The Customer is allowed to use the PSD to produce indicia, which consumes the available postal funds in the PSD. In order to do so he has to perform a "login" into the PSD by presenting a PIN, which identifies him/her (for details see section 3.3.8).

[1] This may take place in the field, but will also be done as the first step in the Return phase.

3.2 Protected Assets

The major asset held in the PSD is the currently available amount of postal funds. Several more objects are identified in order to provide a more detailed picture of the PSD's access control policy.

Table 1: Protected Objects

PSD configuration
Indicia application configuration
Postal funds
Customer attributes
PIN
Statistics and records
Cryptographic keying material

3.2.1 PSD configuration

Hardware and software of the PSD are configured in the manufacturing and initialization phase on ASCOM's premises. The PSD configuration is the hardware and software along with more basic operational parameters and data objects of the PSD in the field [2]. Operational parameters and data objects include 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/software of a PSD 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. The postal funds are decreased every time an indicium is generated and increased by a TMS originated download of new funds.

[2] It is this configuration that is primarily subject to security policy considerations in this document.

3.2.4 Customer Attributes

Various attributes are used to identify and describe the 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 PSD 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 as 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

The indicia are primarily secured by a digital signature generated with a dedicated private key stored in the PSD. Other cryptographic keys are used to authenticate the entities ASCOM CA, ASCOM Regional CA, ASCOM Remote Control and ASCOM Manufacturing. Domain parameters used by any cryptographic mechanisms are also regarded as being a part of the cryptographic keying material[3].

Keys and certificates stored in a PSD consist of:

- ASCOM Root CA certificate,
- ASCOM (Factory Region) Regional CA certificate (temporarily),
- ASCOM Regional CA certificate,
- ASCOM Manufacturing certificate (temporarily),
- ASCOM Remote Control certificate (temporarily),
- PSD Authentication certificate and the corresponding private key,
- Indicia certificate and private key,
- User PIN Keys,
- TMS keys,
- Ephemeral Diffie-Hellman keys (temporarily).

3.3 Services and Access Control Policy

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

Note: This security policy focuses on the PSDs in the field (see sect. 2.4). References to manufacturing related phases (Manufacturing and Initialization) as well as to the Return phase are made here only to provide the reader with a complete picture of the overall life cycle.

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

Table 2: PSD Services

Service	Roles		Access allowed for	Life cycle phase
	C.O.	User		
General Device Initialization	X		ASCOM Manufacturing	Initialization
Customer Specific Initialization	X		ASCOM Remote Control	Authorization
Funds Download		X	TMS	Operation
Indicia Generation		X	Customer	Operation
Generate Indicia Key Pair	X		ASCOM Remote Control (ASCOM Manufacturing)	Authorization (Return)
Get Indicia Public Key	X		ASCOM Remote Control (ASCOM Manufacturing)	Authorization (Return)
Generate Authentication Key Pair	X		ASCOM Manufacturing	Initialization
Get Authentication Public Key	X		ASCOM Manufacturing	Initialization
Generate Diffie-Hellman Key Exchange for TDES Session Key Creation	X	X	ASCOM Manufacturing ASCOM Remote Control TMS	Initialization Authorization Operation
Generate PIN Keys	X	X	ASCOM Manufacturing Customer	Initialization Operation
Generate TMS Keys		X	TMS	Operation
Get Certificates	X		ASCOM Manufacturing ASCOM Remote Control	Initialization Authorization
Log Extraction	X		ASCOM Remote Control (ASCOM Manufacturing)	Operation (Return)
Information	X	X	All	Operation (Return)

Management of Cryptographic Services	X		ASCOM Remote Control (ASCOM Manufacturing)	Operation (Initialization /Return)
Customer Authentication	X	X	Customer (see section 3.3.8) and ASCOM Remote Control	Operation
Enabling/Disabling the PSD	X	X	TMS and ASCOM Remote Control	Operation

3.3.1 General Device Initialization

ASCOM Manufacturing will initialize the PSD 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 PSD as part of the functions related to this service.

ASCOM Manufacturing, in the initialization phase of the PSD, uses certain special diagnostic applications and other initialization applications in order to initialize various data objects and finally to load the indicia application which provides the control for use of the PSD in the field.

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

3.3.2 Customer Specific Initialization

This service includes functions performed by ASCOM Remote Control in the field in order to configure the PSD for the use with a specific customer.

This includes loading of attributes identifying and describing the specific customer. It also includes the setting of values for parameters, which are specific for the customer and are recognized by the indicia application in operation (e.g. limits for new funds).

3.3.3 Funds Download

TMS may access the PSD in the field through the KMS functional entity for downloading of new funds. The communications with the PSD and the related exchange of TMS data is accommodated via the cryptographically secured messaging mechanism specified in section 3.3.7.

TMS carries out the following operations as part of the funds downloading operation:

- 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 PSD allowing TMS to compare it with available information for correctness (“device audit”);
- reads various values and parameters of the PSD configuration, the Indicia application configuration and the customer attributes;

- may modify the PSD's date-and-time;
- releases the PSD for further use.

The PSD tracks the remaining amount of available funds and the total amount of funds used for indicia creation[4].

A PSD internal Watchdog timer is used to automatically inhibit further indicia creations until proper audit is done.

The TMS provides the accounting services necessary to support USPS funds management requirements.

3.3.4 Indicia Generation

The Customer may generate indicia using the available funds [USPS00]. 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 PSD indicia application function is not disabled because of an overdue audit (see section 3.3.3).

3.3.5 Log Extraction

ASCOM Remote Control may extract Statistics and Records from PSDs in the field for diagnostic purposes, while ASCOM Manufacturing may extract this data as part of the Return procedures.

3.3.6 Information

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

Information available includes:

- the current amount of postal funds;
- the value of various application relevant parameters (as applicable limits);
- various attributes identifying and describing the specific customer and the device;
- diagnostics and status information about the PSD device.

3.3.7 Management of Cryptographic Services

ASCOM Manufacturing and ASCOM Remote Control may query and set various elements of the PSD'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:

[4] These values are referred to conceptually as "descending register" and "ascending register", see [USPS00].

- initiate the generation of a PSD authentication key pair in a PSD and get the public key component for certification;
- initiate the generation of the PIN keys used to decrypt the securely transmitted PIN received for Customer authentication to the PSD,
- set and verify cryptographic parameters and certificates.

Available functions for ASCOM Remote Control in the field are:

- initiate the generation of a Indicia key pair in a PSD and get the public key component from the PSD for certification;
- re-keying of a PSD (e.g. initiate the PSD internal generation of a new Indicia key pair);
- PSD log extraction.

The data exchanged for the purpose of the management of cryptographic services is secured using an "authenticated Diffie-Hellman channel" with data integrity protection and symmetric encryption.

The communications protocol used to establish the secure channel provides the following security features:

- replay protection by using random numbers as time variant parameters;
- establishment of shared secret session keys between the two communicating entities by Diffie-Hellman technique;
- mutual control of the shared secret keys;
- forward secrecy for the shared secret session keys (a compromised key does not put at risk future session keys);
- authentication of the communicating parties by the use of digital signatures and certificates;
- encryption and integrity protection through use of symmetric techniques;
- independent cryptographic keys for encryption and integrity protection.

3.3.8 Customer Authentication

The PSD is a single-user device that uses identity-based methods to authenticate its user. The Customer is allowed to use the PSD to produce indicia, which consumes the available postal funds in the PSD. In order to do so, he has to perform a "login" into the PSD by presenting a PIN to identify himself.

The Customer is authenticated using a PIN based mechanism. The PIN is set to a unique PSD individual value in the Manufacturing phase. This value is made known to the customer using a communication path different from the shipping of the PSD itself. The customer is empowered to change the PIN when he uses the PSD the first time.

The PSD expects the customer identity PIN to be entered each time after powering up and before using the customer role. The PSD also expects the PIN authentication procedure to be performed again each time the synchronization at the serial interface between the PSD and the

host system is lost. This event indicates to the PSD that it might have been moved to a different host system.

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

Whenever a specific consecutive number of authentication failures has occurred the PIN authentication function is locked, which effectively prevents the access to the indicia generation. ASCOM Remote Control may reset the PIN to its initial value.

At first power-up of an initialized PSD, the customer enters the PIN through a keypad on the host/base. The host/base then encrypts the PIN and transfers it to the PSD. The Customer is not forced to re-enter the PIN at each power-up since this is the only entity that accesses the module through this interface, in the field.

The PIN is protected by encryption prior to transmission from the host/base to the PSD by symmetric keys. This applies to both the regular entry of the current PIN and to a PIN change. The PIN is never communicated in the clear.

The PIN keys are triple DES keys generated by the PSD and used for secure transmission of the Customer PIN. This process is initially performed in the initialization phase.

3.4 Enabling/Disabling the Postal Security Device (PSD)

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

When the electronic tamper response mechanism is activated the following battery-backed RAM security-critical data elements are destroyed (zeroed) thus making the PSD inoperative:

- ASCOM Root CA certificate,
- ASCOM (Factory Region) Regional CA certificate (temporarily),
- ASCOM Regional CA certificate,
- ASCOM Manufacturing certificate (temporarily),
- ASCOM Remote Control certificate (temporarily),
- PSD Authentication certificate and the corresponding private key,
- Indicia certificate and private key,
- User PIN Keys,
- TMS keys,

4 Key Management

The following cryptographic elements are stored in a PSD:

- ASCOM Root CA certificate,
- ASCOM (Factory Region) Regional CA certificate (temporarily),

- ASCOM Regional CA certificate,
- ASCOM Manufacturing certificate (temporarily),
- ASCOM Remote Control certificate (temporarily),
- PSD Authentication certificate and the corresponding private key,
- Indicia certificate and private key,
- User PIN Keys,
- TMS keys,
- Ephemeral Diffie-Hellman keys (temporarily).

Table 3: Cryptographic elements stored in the PSD

Cryptographic element	Generation	Initialization in PSD	Usage by PSD	Replacement in PSD
ASCOM Root CA certificate	Generated by ASCOM Root CA	*Manufacturing/ initialization* phase	Verification of Regional CA certificates. Verification of signatures on PSD application binaries.	As part of re-keying When Return application is loaded
Ephemeral Diffie-Hellman key pairs	Generated by PSD	*Initialization*/*Authorization/Operation* phase	(Temporarily) Creation of session keys for secure communication with the KMS.	Whenever a secure communication session is created
ASCOM (Factory Region) Regional CA certificate	Issued by ASCOM Root CA	*Manufacturing/ initialization* phase	(Temporarily) Verification of Manufacturing Certs (only Factory Region).	As part of Authorization When Return application is loaded
ASCOM Manufacturing certificate	Issued by ASCOM (Factory Region) Regional CA	*Manufacturing/ initialization* phase	(Temporarily) Verification of ASCOM Manufacturing and signed data of message exchanges with KMS.	As part of Authorization When Return application is loaded
ASCOM Regional CA certificate	Issued by ASCOM Root CA	*Authorization* phase	Verification of Remote Control Certs.	As part of re-keying When Return application is loaded
PSD Authentication key pair	Generated by PSD	*Initialization* phase	Private key signs data of message exchanges with regional KMS	As part of re-keying When return application is loaded
ASCOM Remote Control certificate	Issued by ASCOM Regional CA	*Authorization* phase	(Temporarily) Verification of ASCOM Remote Control and signed data of message exchanges with KMS.	As part of re-keying
Indicia key pair	Generated by PSD	*Authorization* phase	Private key signs indicia data	As part of re-keying When Return application is loaded
TMS keys	Agreed by PSD and TMS	*Operation* phase	Provide mutual authentication of TMS and PSDs and protection of data integrity and confidentiality	As part of every postal funds download operation When Return application is loaded
User PIN Keys	Initially Generated by PSD	*Operation* phase	Logon to PSD	When user enters his/her own PIN

4.1 ASCOM Root CA certificate

The ASCOM Root CA certificate is loaded into each PSD during the Manufacturing/ Initialization phase.

The ASCOM Root CA certificate is self-signed. It contains a hash of the next public key and the associated cryptographic domain parameters.

The security of a subsequent replacement of the ASCOM Root CA Certificate (whether accomplished remotely, in the field, or as part of the return re-manufacturing process) is based on the data origin authentication and integrity protection provided by the hash value (being part of the signed data) stored in the previous version of the ASCOM Root CA certificate.

The ASCOM Root CA private key is applied to issue ASCOM Regional CA certificates and to sign PSD application binaries.

The PSD uses the ASCOM Root CA certificate to verify subsequent ASCOM Regional CA certificates and to check the signature on application binaries to be loaded.

The first time an application is run it is verified against this signature, then a CRC is calculated/stored and all subsequent startups of the application verify this CRC.

4.2 Ephemeral Diffie-Hellman Key Pair

The Diffie-Hellman key pairs are initially created by the PSD during the Manufacturing/ Initialization phase. These keys are used to establish shared secrets for authenticated Diffie-Hellman communication sessions with the KMS for which, data integrity and confidentiality are protected, see section 3.3.7.

4.3 ASCOM (Factory Region) Regional CA certificate

The ASCOM (Factory Region) Regional CA certificate is loaded into each PSD during the Manufacturing/Initialization phase.

The ASCOM (Factory Region) Regional CA certificate is issued by the ASCOM Root CA.

The ASCOM (Factory Region) Regional CA private key is used to issue the following certificates:

- ASCOM Manufacturing certificates;
- PSD Authentication certificates.

The PSD uses the ASCOM (Factory Region) Regional CA certificate to verify the ASCOM Manufacturing certificate and thus the corresponding role.

The ASCOM Regional CA certificate is only temporarily stored in the PSD and is replaced during the Authorization phase by the ASCOM Regional CA certificate when the PSD is sent to a destination in the field.

4.4 ASCOM Manufacturing certificate

The ASCOM Manufacturing certificate is loaded into each PSD during the Manufacturing/ Initialization phase.

The ASCOM Manufacturing certificate is issued by the ASCOM (Factory Region) Regional CA.

The ASCOM Manufacturing private key is used to sign messages sent by ASCOM Manufacturing to the PSD. The PSD uses the ASCOM Manufacturing certificate to verify the ASCOM Manufacturing role and any signed messages sent by the entity. The ASCOM Manufacturing certificate is only temporarily stored in the PSD and is replaced during the Authorization phase by the Remote Control certificate when the PSD is sent to a destination in the field.

4.5 ASCOM Regional CA certificate

The ASCOM Regional CA certificate is loaded into each PSD during the Authorization phase[5].

The ASCOM Regional CA certificate is issued by the ASCOM Root CA.

The ASCOM Regional CA private key is used to issue the following certificates:

- ASCOM Remote Control certificates;
- PSD Authentication certificates.

The PSD uses the ASCOM Regional CA certificate to verify the ASCOM Remote Control certificate and thus the corresponding role.

In the field, ASCOM Remote Control may initialize a replacement of the ASCOM Regional CA certificate in a specific PSD as part of a re-keying operation. This operation is integrated in an authenticated Diffie-Hellman communication session for which, in addition, data integrity and confidentiality are protected, see section 3.3.7.

The ASCOM Regional CA certificate contains a Region Code that controls when a new regional certificate can replace an existing regional certificate in a PSD.

4.5.1 Region Codes

A Region Change procedure is used to reconfigure a PSD when it moves from one region to another.
Each ASCOM Regional CA certificate will contain two region codes, the "Active Region Code" and the "Prior Region Code". These region codes act as constraints on the certificate change process to provide the ability to configure a PSD to its regional certificate hierarchy, reconfigure a returned PSD for ASCOM manufacturing, and not allow a regional KMS to reconfigure a PSD for a different region, cf. section 3.1.2.

4.6 PSD Authentication Key Pair

The PSD Authentication key pair is generated by the PSD itself. This process is performed during manufacture of a PSD.

[5] The ASCOM Regional CA certificate replaces the ASCOM Manufacturing certificate already stored in each PSD.

The public key is extracted by ASCOM Manufacturing and transferred to the ASCOM Regional CA (of the Factory Region) for certification.

The PSD Authentication private key is used to sign responses by a PSD to ASCOM Manufacturing and Remote Control messages.

In the field, ASCOM Remote Control may initialize a replacement of the PSD Authentication key pair as part of a re-keying operation. This is done by first instructing the PSD to generate a new key pair. As a result ASCOM Remote Control receives the public key part and transfers it to the ASCOM Regional CA for certification. After receiving the certified public key back, ASCOM Remote Control will instruct the PSD to switch from the old key to the new one, which will be used from then on to authenticate the PSD to the regional KMS. This operation is integrated in an authenticated Diffie-Hellman communication session for which, in addition, data integrity and confidentiality are protected.

4.7 ASCOM Remote Control certificate

The ASCOM Remote Control certificate is loaded into each PSD during the Authorization phase.

The ASCOM Remote Control certificate is issued by the ASCOM Regional CA.

The ASCOM Remote Control private key is used to sign messages sent by ASCOM Remote Control to the PSD. The PSD uses the ASCOM Remote Control certificate to verify the ASCOM Remote Control role and any signed messages sent by the entity.

The ASCOM Remote Control certificate is only temporarily stored in the PSD. In the field, ASCOM Remote Control may initialize a replacement of the certificate as part of a re-keying operation. This operation is integrated in an authenticated Diffie-Hellman communication session for which, in addition, data integrity and confidentiality are protected, see section 3.3.7.

4.8 Indicia Key Pair

The Indicia key pair is generated by the PSD itself. This process is performed in the field during the Authorization phase.

The public key is extracted by ASCOM Remote Control and transferred to USPS IBIP key management infrastructure for certification.

The Indicia private key is used to sign indicia data.

In the field, ASCOM Remote Control may initialize a replacement of the Indicia key pair (re-keying). This is done by first instructing the PSD to generate a new Indicia key pair. As a result ASCOM Remote Control receives the public key part and transfers it the same way as in the initialization phase to the USPS IBIP key management infrastructure for certification. After receiving the certified public key back, ASCOM Remote Control will instruct the PSD to switch from the old Indicia key to the new one, which will be used from then on for indicia generation. This operation is integrated in an authenticated Diffie-Hellman communication session for which, in addition, data integrity and confidentiality are protected.

4.9 TMS Keys

The TMS keys are symmetric keys used to mutually authenticate TMS and PSDs and to protect the integrity of the data exchange during a postal funds download operation.

The TMS keys are session keys agreed upon by a specific PSD and TMS as part of every PSD reset operation.

The TMS related data exchange is embedded in an authenticated Diffie-Hellman communication session for which data integrity and confidentiality are protected.

4.10 User PIN Keys

The generation of the PSD specific initial PINs takes place during the PSD initialization step on Ascom's premises. The PSD itself internally generates its initial PIN using the ANSI X9.17 PRNG. After having generated the random bits followed by some formatting the PSD outputs the initial PIN to the Ascom KMS, which stores the value in a database.

4.11 Random Number Generation

The PSD uses a ‘true’ random number generator to seed its FIPS-approved ANSI X9.17 pseudo random number generator. The output of this PRNG is used for key generation by the PSD.

5 Annexes

5.1 References

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

[USPS00] United States Postal Service (USPS): Information-Based Indicia Program (IBIP) : Performance criteria for information-based indicia and security architecture for IBI postage metering systems. February 23, 2000 – Draft

5.2 Acronyms

CA	Certification Authority
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
FIPS PUB	Federal Information Processing Standard Publication
IBI	Information Based Indicia
IBIP	Indicia Based Information Program
PCB	Printed Circuit Board
PIN	Personal Identification Number
PSD	Postal Security Device
TMS	TeleMeter Setting System