Postage Meter Approval Protection Profile

Authors	Kevin Appleford Steve Hill
Reporting to	Deborah Moir
Valid on	30 April 2001
Status	Definitive
Deliverability	EXTERNAL
File number	CLEF.25885.40.1
Issue Number	1.1
Page count	81

Signed (Authors)

Authorised

TABLE OF CONTENTS

REFERENCES

CC — Common Criteria for Information Technology Security Evaluation (Comprising Parts 1-3, [CC1], [CC2], [CC3]).

CC1 — Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and General Model
CCIMB-99-031, Version 2.1, August 1999.

CC2 — Common Criteria for Information Technology Security Evaluation
Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999.

CC3 — Common Criteria for Information Technology Security Evaluation
Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999.

CEM — Common Methodology for Information Technology Security Evaluation
Part 2: Evaluation Methodology,
CEM-99/045, Version 1.0, August 1999.

IPMAR — International Postage Meter Approval Requirements
Universal Postal Union Technical Standards Manual S30-3,
1 February 2000.

1. INTRODUCTION

1.1 PP Identification

Title: Postage Meter Approval Protection Profile

Authors: Kevin Appleford and Steve Hill

File Number: CLEF.25885.40.1

Publishing Date: 30 April 2001

Issue Number: 1.1

Sponsoring Organisation: Royal Mail

Version of CC used for development: CC Version 2.1 (also known as ISO 15408).

This protection profile has been developed to identify and describe the security requirements needed as a basis for the approval of postal meters within a Common Criteria framework consistent with the International Postage Meter Approval Requirements of the Universal Postal Union (UPU) [IPMAR].

1.2 PP overview

The Target of Evaluation (TOE) for this protection profile is a Postage Meter.

Postage meters provide mechanisms for metering postal funds, and for identifying the valid use of postal services via the issuing of receipts for these services in the form of printed indicia (postal franking).

The value of the postal funds within a meter may represent either the purchased postage value that has been bought and downloaded to the meter and that remains to be used, or the total postage value that has been used for postal services but that remains to be paid. This metered value is held within the revenue sensitive registers of the postal meter. The security functionality of a postal meter seeks to protect the integrity of this value and the confidentiality and integrity of security sensitive parameters necessary to support the protection of the TOE and the transfer of value between the meter and its supporting postal authority.

Attacks on postal meters may be to try to alter or corrupt the revenue sensitive elements to gain value or to obtain services without the correct metering. These attacks may target the meter itself, or may target the indicia

belonging to a postage meter allowing services to be fraudulently obtained via some counterfeiting of the indicia.

The scope of this Protection Profile (PP) is consistent with the International Postage Meter Approval Requirements of the UPU [IPMAR], and covers those general security needs that the UPU considers are necessary for its approval of the security of new postage meters.

This PP covers, in particular, functional requirements in the following domains:

- the physical security of the meter against probing and tampering including electromagnetic interference/compatibility issues,
- the software security of the postage metering application software,
- the software security of any underlying operating system,
- the software services that an underlying operating system may offer,
- the authorised roles and services,
- cryptographic key management,
- cryptographic algorithms.

This PP also identifies assurance requirements that cover characteristics of the design and implementation, and documentation of postage meters deemed necessary within the international postage meter approval process; e.g. the use of Finite State Machine models to document and characterise the meter.

1.3 CC Conformance

This PP is Part 2 conformant and Part 3 augmented for EAL4.

1.4 Scope

The structure of this document is as defined by [CC] Part 1 Annex C.

- Section 2 is the TOE Description.
- Section 3 provides the statement of TOE security environment.
- Section 4 provides the statement of security objectives.
- Section 5 provides the statement of IT security requirements.
- Section 6 provides the Operating System Functional Package.

- Annex A provides the security objectives, security requirements and TOE summary specification rationales.
- Annex B provides a correlation table between the IPMAR requirements and the CC security functional requirements and security assurance requirements of this PP.

1.5 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

***Accounting data*:** any record of revenue available, held, used or transferred to a revenue-sensitive module.

***ANSI*:** American National Standards Institute.

***Automated key distribution*:** the distribution of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., down-line key loading, the automated key distribution protocols of ANSI X9.17).

***Categories of error state*:** there are three states - user reset, engineer only reset, and not possible to reset. All error states shall be able to be reset to an acceptable operational or initialisation state except for those hard errors which require maintenance, service or repair of the module.

***Compromise*:** the unauthorised disclosure, modification, substitution or use of sensitive data (including plain text cryptographic keys and other critical security parameters).

***Confidentiality*:** the property that sensitive or private information is not disclosed to unauthorised individuals, entities or processes.

***Control information*:** information that is entered into a revenue-sensitive module for the purposes of directing the operation of the module.

Critical security parameters*:** security-related information (e.g., cryptographic keys, resetting codes, authentication data such as passwords and PlNs) appearing in plain text or otherwise unprotected form and whose disclosure or modification can compromise the security of a revenue-sensitive module or the security of the information protected by the module. For any given design implementation of a postage meter some critical security parameters, e.g. public cryptographic keys, authentication signatures, value registers, etc., may not be regarded as "secret" critical security parameters and may therefore be exempt from the explicit requirements associated with the clearing, or **zeroisation** process, which protects critical security parameters from exposure. ***NOTE: A Security Target claiming conformance to this Protection Profile will need to refine this definition to identify the critical security parameters specific to that TOE.

***Critical security parameter entry states*:** states for entering cryptographic keys and other critical security parameters into the module, and for checking their validity.

***Cryptographic key (key)*:** a parameter used in conjunction with a crypto-graphic algorithm that determines, for example:

- the transformation of plain text data into ciphertext data;
- the transformation of ciphertext data into plain text data;
- the transformation of accounting data;
- a digital signature computed from data;
- the verification of a digital signature computed from data;
- a data authentication code (DAC) computed from data.

***Cryptographic key component (key component)*:** for example, a parameter which is combined via a bit-wise exclusive-OR operation with one or more other identically sized key component(s) to form a plain text cryptographic key.

***Cryptographic module*:** the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and shall be contained within the revenue-sensitive boundary of a meter's revenue-sensitive module.

***Crypto-officer role*:** the distinct authorised but optional role in which an individual or system (e.g. remote meter inspection system) performs functions associated with critical security parameters (non-revenue related), e.g. cryptographic initialisation and key management.

***Cumulative register**:* the register which records the total value used by the meter to date.

***DAC*:** see "Data Authentication Code".

***Data authentication code (DAC)*:** a cryptographic checksum, e.g. based on DES (see FIPS PUB 113); also known as a Message Authentication Code (MAC) in ANSI standards.

***Data key*:** a cryptographic key which is used to cryptographically process data (e.g., encrypt, decrypt, sign, authenticate).

***Data path*:** the physical or logical route over which data passes; a physical data path may be shared by multiple logical data paths. Where a revenue-sensitive module incorporates a printer for producing reports or indicia, the printer is an output data path whose internal design has to be considered and described from the perspective of offering additional data paths e.g. to change the content of indicia.

***DES*:** Data Encryption Standard (see FIPS PUB 113).

***Digital signature*:** a non-forgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.

***EDC*:** see "Error Detection Code".

***EFP*:** see "Environmental Failure Protection".

***EFT*:** see "Environmental Failure Testing"

***Electromagnetic compatibility (EMC)*:** the ability of electronic systems to operate in their intended environments without suffering an unacceptable degradation of the performance as a result of unintentional electromagnetic radiation or response.

***Electromagnetic interference (EMI)*:** electromagnetic phenomena which either directly or indirectly can contribute to a degradation in the performance of an electronic system.

***Electronic key entry*:** the entry of cryptographic keys into a revenue-sensitive module in electronic form, using a key loading device. The user entering the key shall have no knowledge of the plain text value of the key being entered.

***EMC*:** see "Electromagnetic compatibility".

***EMI*:** see "Electromagnetic interference".

***Encrypted key (ciphertext key)*:** a cryptographic key that has been encrypted with a key encrypting key, a PIN or a password in order to disguise the value of the underlying plain text key.

***Environmental failure protection (EFP)*:** the use of features designed to protect against a compromise of the security of a revenue-sensitive module due to environmental conditions or fluctuations outside of the module's normal operating range.

***Environmental failure testing (EFT)*:** the use of testing to provide a reasonable assurance that a revenue-sensitive module will not be affected by environmental conditions or fluctuations outside of the module's normal operating range in a manner that can compromise the security of the module.

***EPROM*:** Erasable Programmable Read-Only (Non-volatile) Memory.

***EEPROM (E^2PROM)*:** Electronically-Erasable Programmable Read-Only (Non-volatile) Memory.

***Error detection code (EDC)*:** a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

Error states: states when the module has encountered an error (e.g., failed a self-test, attempting to encrypt while missing operational keys or other critical security parameters, or cryptographic errors).

***Finite state machine model (FSMM)*:** a mathematical model of a sequential machine which is comprised of a finite set of states, a finite set of inputs, a finite set of outputs, a mapping from the sets of inputs and states into the set of states (i.e. state transitions), and a mapping from the sets of inputs and states onto the set of outputs (i.e. an output function).

***FIPS*:** Federal Information Processing Standard of the United States of America.

***FIPS PUB*:** FIPS Publication.

***Firmware*:** the programmes and data (i.e. software) permanently stored in hardware (e.g., in ROM, PROM, or EPROM) such that the programmes and data cannot be dynamically written or modified during execution. Programmes and data stored in EEPROM are considered software.

***FSM*:** Finite State Machine *(see "Finite state machine model").*

***Hard Error states*:** states which consist of both errors indicating an equipment malfunction and errors requiring maintenance, service or repair of the module. (Hard error states may occur after an identifiable number, combination or sequence of related but otherwise recoverable "soft" errors).

***Hardware*:** the physical equipment used to process programmes and data in a cryptographic module.

***High level language*:** computer programming language with comprehensive support for symbol names, application-oriented commands, stylised programme structure, and controlling the flow of programme execution – designed to support efficient programme development and easy programme maintenance.

***IC*:** Integrated Circuit.

***Indicia*:** the printed output of a postage meter (e.g. a frank) – identifying or authenticating the value of a service or transaction.

***Initialisation vector (IV)*:** a vector used in defining the starting point of an encryption process within a cryptographic algorithm (e.g. the DES Cipher Block Chaining mode of operation as specified in FIPS PUB 81).

***Input data*:** information that is entered into a revenue-sensitive module for the purposes of transformation or computation.

***Integrity*:** the property that sensitive data has not been modified or deleted in an unauthorised and undetected manner.

***Interface*:** a logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.

***ISO*:** International Organisation for Standardisation.

***IV*:** see "Initialisation Vector".

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key loader: a self-contained unit which is capable of storing at least one plain text or encrypted cryptographic key or key component which can be transferred, upon request, into a revenue-sensitive module.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, counters) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

MAC: Message Authentication Code (see "Data Authentication Code").

Maintenance access interface: the combination of physical and logical design elements that enable and support the legitimate maintenance, testing, servicing or repair of the revenue-sensitive module.

Manual key distribution: the distribution of cryptographic keys, often in a plain text form requiring physical protection, but using a non-electronic means, such as a bonded courier.

Manual key entry: the entry of cryptographic keys into a revenue-sensitive module from a printed form, using devices such as buttons, thumb wheels or a keyboard.

Microcode: the elementary computer instructions that correspond to an executable programme instruction.

Operator: an individual accessing a revenue-sensitive module, either directly or indirectly via a process operating on his or her behalf, regardless of the specific role the individual assumes.

Output data: information that is to be output from a revenue-sensitive module that has resulted from a transformation or computation in the module. Where a revenue-sensitive module incorporates a printer for producing reports or indicia, the printed reports and indicia are output data and the printer is an output data path.

Password: a string of characters used to authenticate an identity or to verify access authorisation.

PC: personal computer.

Personal Identification Number (PIN): e.g. a 4 to 12 character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a revenue-sensitive module or of cryptographic keys or other critical security parameters using physical means.

PIN: see “Personal Identification Number”.

Plain text key: an unencrypted cryptographic key which is used in its current form.

Port: a functional unit of a revenue-sensitive module through which data or signals can enter or exit the module. Physically separate ports do not share the same physical pin or wire.

Postage meter: a machine which prints indicia (a franking machine) or similar for metering or issuing a receipt for postal funds or services. It consists of a single revenue sensitive module or contains secure elements that are the revenue sensitive modules of the postage meter.

Postal authority: an agency recognised by the UPU which has the ability to administer, sell or perform postal services.

Power on/off states**:** states for primary, secondary, or backup power. These states may distinguish between power applied to different portions of the module.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Programme image: the full set of objects (executable code, data, etc.) that are required to perform the whole task(s) for which the programme was designed.

PROM: programmable read-only (non-volatile) memory.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public.

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted party.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

RAM: Random Access Memory (volatile memory).

Real time clock: a device which keeps track of the date and time.

Recoverable soft error states: states that may require initialisation or resetting of the module.

Remaining credit register: a register which determines the purchased postage value that remains unused. If postage is to be paid for after use, the register uses the "credit arranged" value instead of the purchased value.

Resetting: a procedure (perhaps secured by one or a combination of a password, PIN, authentication of encrypted data or physical device) which transforms the amount of revenue available or held within a revenue-sensitive module – and hence the revenue due to a postal authority.

Revenue officer role: the distinct authorised role in which an individual or system (e.g. remote meter resetting system) performs functions associated with revenue-related critical security parameters such as resetting, auditing, or revenue-related cryptographic initialisation and key management.

Revenue-officer: The role assumed by an authorised officer performing a set of cryptographic initialisation or management functions (such as meter resetting, modifying accounting data, cryptographic key and parameter entry, cryptographic key cataloguing, audit functions, and alarm resetting).

Revenue officer states**:** states in which an individual or system (e.g. remote meter resetting system) performs functions associated with revenue e.g. resetting, auditing, or revenue-related cryptographic initialisation and key management.

Revenue-sensitive boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a revenue-sensitive module.

Revenue-sensitive module: a part of a postage meter that contains, transmits or receives information or codes that are relevant to the revenue of a postal authority.

Revenue-sensitive module security policy: a precise specification of the security rules under which revenue-sensitive modules must operate, including the security rules derived from the requirements of this standard and any additional security rules imposed by the vendor.

Revenue-sensitive printing system: is a printing system associated with a revenue-sensitive module, which generates a printed output, such as an indicia, that is physical proof of the purchase of goods or services.

ROM: read-only memory (non-volatile memory).

RSM: see "Revenue-sensitive module".

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level; rather, it implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single, secure key for both encryption and decryption.

Security policy: see “Revenue-sensitive module security policy”.

Self-test states: states for performing self-tests on the module (see section 6.11, "Self-Tests").

Software: the programmes, and possibly associated data, that can be dynamically written and modified.

Split knowledge: a condition under which two or more entities separately have key components which individually convey no knowledge of the plain text key which will be produced when the key components are combined in the revenue-sensitive module.

Status information: information that is output from a revenue-sensitive module for the purposes of indicating certain operational characteristics or states of the module.

System software: the special software (operating system, compilers or utility programmes) assigned for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, programmes, and data.

Trusted path: a mechanism by which a person or process can communicate directly with a revenue-sensitive module and which can only be activated by the person, process or module, and cannot be imitated by untrustworthy software within the module.

UPU: Universal Postal Union.

User role: The role assumed by an authorised user obtaining security services, performing revenue-sensitive operations, or other authorised functions. The user role may be the default role for the meter after power-up tests have been successfully completed, or any other role has been successfully relinquished.

User service states*:* states in which authorised users obtain security services, perform cryptographic operations, or perform other authorised user functions.

Zeroisation: a method of erasing, or clearing, electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. In the context of IPMAR, zeroisation is only likely to be applicable to those critical security parameters that are "secret". Zeroisation is unlikely to be a requirement for those critical security parameters for which "integrity" is the fundamental requirement e.g. value-registers; however, it may be applicable to any cryptographic key that is used to authenticate the integrity of a value-register. The scope of zeroisation may be relevant to a postage meter's ability to deliver an authenticated audit trail of the services and errors recorded by the meter even after zeroisation has been performed.

2. TOE DESCRIPTION

2.1 Intended Use

The primary purpose of postage meters is the dispensation and accounting of postal services via postage indicia, and the primary user operation is the request for such service. Meters, at the very least, are able to provide basic accounting information, and the protection of the integrity of such information.

It may be the case that many other aspects connected with, but peripheral to this function, may also be performed by such meters, for example letter folding. Postage meters have a wide range of potential user functionality which reflects their use in servicing the diverse needs of large to small business enterprises.

Notwithstanding the complexity of the user operations that a postage meter may perform, all postage meters provide some basic security services to safeguard the revenue aspects of their processing, this is the postage metering aspect. It is performance and the security of these revenue aspects by information technology, and the consequent protection needed for the aspects of the security solution, itself, that is addressed by this protection profile. This is particularly with respect their access by persons in particular roles for example ordinary users or revenue officers, and the integrity of the information via cryptographic operations on such data.

The administration, the sale and actual performance of the postal service are through the agency of a postal authority, and it is the postal authority's value that is being protected by the security of the postage meter and its associated indicia.

Postage metering also takes place in a wide range of environments which may be open to physical attacks using sophisticated test equipment and probing on the one hand, or via Internet connections and attacks from hackers and hacker groups on the other hand. Attackers may have in-depth understanding of the operating systems on which metering applications may rely, and may be well funded, well resourced and well motivated. This protection profile provides various levels of countermeasure to such attacks through increasing strength against physical attack, and by the increasing sophistication of the underlying IT system.

2.2 Security Features

Attacks on postal meters comprise:

- attacks on the revenue sensitive elements or on critical security data so as to fraudulently obtain postal services, which might involve attacks on the physical or logical characteristics of the meter; or
- attacks on the indicia, belonging to a postal authority and identifying the postage meter and service characteristics, allowing services to be fraudulently obtained via some counterfeiting of the indicia.

The countermeasures that this PP identifies include:

- Physical tamper protection and detection;
- Management and protection of Cryptographic keys - the keys themselves might be used to ensure:
    - the confidentiality of entities: e.g. application and operating system software, the downloading of value to the meter, confidentiality and integrity of messages between the meter and a postal authority,
    - integrity of entities: e.g. application and operating system software, the downloading of value to the meter, revenue sensitive values,
    - authentication services: e.g. authenticating both the meter and a postal authority and other entities to each other, ensuring that counterfeit indicia can be identified,
    - non-repudiation services: e.g. ensuring that postal value is correctly accounted by distinguishing genuine indicia;
- Split knowledge and dual control, protecting keys that should be known only to a postal authority;
- Access controls to data provided by the operating systems;
- The use of authorised roles and services to uphold the separation of duties and principle of least privilege;
- Authentication services to authenticate users and their roles.

The scope of this Protection Profile (PP) is consistent with the International Postage Meter Approval Requirements (IPMAR) of the UPU, and covers

those general security needs that the UPU considers are necessary for its approval of the security of any postage meters

3. TOE SECURITY ENVIRONMENT

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

To this end, the statement of TOE security environment identifies and lists the assumptions made on the environment and the intended method of use of the TOE, defines the threats that the TOE is designed to counter, and the organisational security policies with which the TOE is designed to comply.

3.2 Environmental and Method of Use Assumptions

This section describes the assumptions about the environment in which the TOE is to be used and its intended method of use.

[A.Em] It is assumed that appropriate consideration shall have been given to the design issues associated with EMI/EMC within the meter, in particular the EMI/EMC of the meter shall comply with the national legislation for such meters.

[A.No_Evil] It is assumed that there are one or more individuals who are assigned to administer the TOE. These individuals are not collectively careless, wilfully negligent or hostile.

The individuals assigned to administer the TOE are in normal circumstances assumed to be sufficiently careful, diligent and trustworthy, however in regard to operations involving some critical security data, such as secret or private cryptographic keys authenticating a postal authority, and where this data may be intercepted by such individuals, this assumption does not hold and reliance must be placed on the group actions of such individuals using split knowledge.

3.3 Assumed Threats

This section describes the threats to the assets that require protection.

3.3.1 Assets

The postage meters are intended to be used in potentially hostile user environments.

The primary assets of concern to this PP are the revenue sensitive assets of the TOE (which form at least in part the input and output to cryptographic functions of the TOE).

Secondary assets whose confidentiality and integrity must be protected consist of characteristics of the TOE important for the security of the system. These assets include:

- non-cryptographic critical security parameters e.g. for identification and authentication such as password or PINs,
- cryptographic keys used by the security processes of the TOE,
- the hardware and firmware upon which the security of the TOE relies,
- the software implementation upon which the security of the TOE relies.

3.3.2 Threat Agents

The threat agents can be categorised as:

- authorised users of the TOE (those users who have some authorisation to use the TOE),
- unauthorised users of the TOE.

When the threat may be come from either authorised or unauthorised users these are simply called attackers. Authorised users may perform in various roles: ordinary users, revenue officers, maintenance officers etc.

Attackers are assumed to have various levels of expertise, motivation and resources. Expertise could be in non-destructive testing, software engineering, the TOE itself or hacking. Their motivation would most likely arise from economic reward. Resources may range from personal computers to sophisticated detection, test and measurement equipment.

3.3.3 Threats

The TOE may be subject to a number of threats against the confidentiality and integrity of its data, software, and services. The attacks may be against the physical, logical or software characteristics of the TOE.

[T.Access] An attacker may try to gain access to services or information protected by the TOE for which he is not authorised.

This consists of unauthorised user trying to access any elements of the TOE, for which they have no authorisation.

[T.Authority] An attacker may try to impersonate an authorised user (or operational group) of the TOE thereby gaining unauthorised access to the TOE and thus to information or services of the TOE.

[T.Counterfeit] An attacker may be able to gain access to the postal services of the TOE by counterfeiting postal indicia.

If the duplication of indicia is a supported function of the TOE, it will be necessary for the evaluation of that TOE to confirm that such functionality does not introduce any vulnerabilities through helping an attacker realise this threat.

[T.Integrity] An attacker may try to modify services or information protected by the TOE for which he is not authorised.

This may be an unauthorised user trying to modify any elements of the TOE, or authorised users trying, for example, to modify revenue-sensitive data, program images, cryptographic parameters, or other critical security parameters of the TOE for which they have no authorisation.

[T.Masquerade] An attacker gains access to services or information protected by the TOE by masquerading as a postal authority.

[T.Non_Secure] An attacker may try to force the TOE into a non-secure state by causing the TOE to error or reset.

[T.Postal_Authority_Access] An attacker may try to access information protected by the TOE which is reserved exclusively to a postal authority.

Certain cryptographic information may be reserved only to a postal authority. Such key information may nevertheless need to be input or output from the TOE via persons other than a postal authority.

[T.Probe] An attacker may try to perform passive probing of the TOE to reveal design or operational content.

Physical probing may consist of attempts to ascertain the internal physical representation of the TOE by looking inside the enclosures of the TOE via the ventilation openings. The goal of the attack would be to identify aspects of the hardware and software security design, and to infer parameters and initialisation data such as passwords, cryptographic keys and identification data which might be available on internal data paths or in registers.

[T.Role] An authorised user of the TOE may try to access information or services protected by the TOE which are reserved to another authorised role for which he has no authorisation.

This consists of authorised users trying, for example, to access revenue-sensitive data, program images, cryptographic parameters, or other critical security parameters of the TOE for which they have no authorisation.

[T.Stress] An attacker may try to gain or modify information protected by the TOE for which he is not authorised by subjecting it to environmental stress.

The attacker subjects the TOE to an abnormal environment, e.g. changes to the temperature or voltage or EM radiation, whilst physically probing the TOE for leaked information or in an effort to affect the integrity of information.

[T.Tamper] An attacker may try to actively interfere with the TOE to cause the TOE to perform outside of its design or to reveal operational content.

An attacker subjects the TOE or components of the TOE to physical action, e.g. forcing access covers off in an effort to then compromise the TOE, rather than passively probing.

3.4 Organisational Security Policies

The TOE must comply with the following organisational security policies:

[P.Accountable] The users of the system shall be held accountable for their actions within the system.

[P.Ac] The right to access postal services of the postal meter shall be determined by the Postal Meter Service access control policy based on:

- the value of the cumulative register; and
- the value of the remaining credit register; and
- the value of the requested service.

The right to postal services shall depend on whether there are sufficient funds or credit remaining to pay for the requested service.

[P.Crypto] The cryptographic key management, key operations and algorithms used by the TOE shall comply with postal authority approved standards.

4. SECURITY OBJECTIVES

4.1 Security Objectives to be met by the TOE

The objectives which are to be met by the TOE are:

[O.Access] The TOE must provide the means for controlling and limiting the access of users and any associated subjects to those objects, resources and services for which they are responsible on the basis of individual users (or groups of users acting in a common role), and in accordance with the rules defined by the TOE's access control policies.

[O.Audit] The TOE must provide the means of recording security relevant events, so as to:

- assist Revenue officers in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack; and

- hold users (or groups of users acting in a common role) accountable for any actions they perform that are relevant to security.

[O.Crypto] The TOE must support cryptographic functions in a secure manner in accordance with the rules defined by P.Crypto, the cryptographic key management and algorithm policies of the TOE, and support the embedding of cryptographic signatures in postal indicia.

The key management aspects of distribution, entry, output, and destruction, and the key operation of private or authenticated data transfer are subject to postal authority approved standards. Key generation however, although necessary for the TOE is not a requirement necessarily met by the TOE.

[O.Enforcement] The TOE must ensure that the security policies enforced by the TSF are not bypassed.

[O.Failsafe] The TOE should preserve a secure state in the event of an error or reset.

[O.IA] The TOE shall identify all users either in a role or individually, and shall authenticate a user in a role before he may take on the claimed role, and before allowing access to the TOE and its resources.

The system does not have to identify individual users if role based access is used.

[O.Integrity] The TOE must provide functionality to detect the loss of integrity of critical data and revenue sensitive software images.

[O.Manage_Maintenance] The TOE must provide functionality which enables authorised maintenance officers to effectively manage the maintenance functionality of the TOE, and must ensure that only authorised maintenance officers are able to access such functionality.

[O.Manage_Revenue] The TOE must provide functionality which enables authorised revenue officers to effectively manage the revenue sensitive security and cryptographic security functionality of the TOE, and must ensure that only authorised revenue officers are able to access such functionality.

[O.Path] The TOE must provide users with secure communications to the TSF.

[O.Probe] The TOE should protect itself and its assets from physical probing.

The TOE must prevent attackers from using any ventilation openings, there might be, to passively probe the postal meter thus compromising the TOE.

[O.Stress] The TOE should protect itself and its assets from environmental stress.

The TOE must be safeguarded to prevent attackers subjecting it to environmental conditions outside the normal range in an effort to compromise the security of the TOE, e.g. exposing it to physical shock or electromagnetic radiation.

[O.Tamper] The TOE should protect itself and its assets from unauthorised physical tampering.

The TOE must be safeguarded to prevent physical interference with the TOE, e.g. breaking into the enclosing housing of the TOE leaving the assets of the TOE available to inspection or modification.

The following security objective is to be satisfied by the TOE in the event that it provides a means by which operators can load and execute software or firmware that is not part of the TOE. (This leads to the *Operating System* functional package requirements as articulated in section 6.)

[O.Label] The TOE shall provide sensitivity labels for revenue-sensitive software, critical security parameters, control and status information, and shall control access to such information on the basis of the sensitivity labels and assigned subject clearances.

4.2 Security Objectives to be met by the TOE Environment

[OE.Admin] Those responsible for the TOE shall establish and implement procedures for training and vetting administrators of the TOE, in particular the revenue officers of the TOE.

[OE.Audit] The revenue officers must ensure that the audit functionality is used and managed effectively.

[OE.Em] Those responsible for the design of the TOE shall give appropriate consideration to the design issues associated with EMI/EMC within the meter, in particular so that the EMI/EMC of the meter shall comply with the national legislation for such meters.

[OE.Key_Generation] The IT environment shall provide an approved method for generating cryptographic keys.

[OE.IA] The revenue officers of the TOE must ensure that authentication data is not disclosed to unauthorised individuals.

[OE.Postal_Authority] The postal authorities must maintain the security of their cryptographic keys, and must ensure that only authentic certificates for the postal authorities are loaded to postal meters.

5. SECURITY REQUIREMENTS

5.1 TOE Security Functional Requirements

This section identifies the security functional requirements (SFRs) required of the TOE to meet its security objectives.

The components taken from [CC2] to specify the SFRs are listed in the table below together with an indication of whether the components are *iterated* (indicated by "(*N)" where N identifies the number of iterations) or *refined*.

Assignment and selection operations to be completed by the ST author are indicated using the same notation as used in [CC2]. Partially completed operations are denoted by *italicisation* of the word *assignment* or *selection* (as appropriate). Completed assignment and selection operations are indicated by *italicised text*. Refinements of components are indicated by **emboldened text**.

CLASS	FAMILY	COMPONENT	REFINED?
FAU	FAU_GEN	FAU_GEN.1	
FCS	FCS_CKM	FCS_CKM.2	
		FCS_CKM.3 (*2)	
		FCS_CKM.4	
	FCS_COP	FCS_COP.1	
FDP	FDP_ACC	FDP_ACC.1	
	FDP_ACF	FDP_ACF.1	
	FDP_DAU	FDP_DAU.1 (*2)	
	FDP_IFC	FDP_IFC.1	
	FDP_IFF	FDP_IFF.1	
	FDP_ITT	FDP_ITT.1	Y
		FDP_ITT.3	Y
	FDP_RIP	FDP_RIP.1 (*2)	Y

CLASS	FAMILY	COMPONENT	REFINED?
FIA	FIA_UAU	FIA_UAU.2	
		FIA_UAU.6	
	FIA_UID	FIA_UID.2	
FMT	FMT_MOF	FMT_MOF.1	
	FMT_MSA	FMT_MSA.1	
		FMT_MSA.2	
	FMT_MSA	FMT_MSA.3	
	FMT_MTD	FMT_MTD.1 (*3)	
	FMT_SMR	FMT_SMR.2	
FPT	FPT_AMT	FPT_AMT.1	
	FPT_FLS	FPT_FLS.1	
	FPT_PHP	FPT_PHP.1	Y
		FPT_PHP.3 (*3)	Y
	FPT_RCV	FPT_RCV.1	Y
	FPT_RVM	FPT_RVM.1	Y
	FPT_SEP	FPT_SEP.1	
	FPT_STM	FPT_STM.1	
	FPT_TST	FPT_TST.1	
FTP	FTP_TRP	FTP_TRP.1	Y

Table 1 - Security Functional Requirements in the core model

5.1.1 FAU - Security Audit

5.1.1.1 FAU_GEN - Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *minimum, basic, detailed, no specifie*d] level of audit; and

c) *Error events and the invocation of critical functions and services; and*

d) *Entry of cryptographic keys and other critical security parameters; and*

e) *Control inputs and status outputs.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant informatio*n].

5.1.2 FCS - Cryptographic Services

5.1.2.1 FCS_CKM.1 - Cryptographic key generation

This PP does not mandate that the TOE provides cryptographic key generation functionality. This is identified as a security requirement for the IT environment (see section 5.3). Nonetheless a conformant TOE may satisfy this requirement.

5.1.2.2 FCS_CKM.2 - Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [*assignment: approved cryptographic key distribution method*] that meets the following: [*assignment: list of approved standards*].

5.1.2.3 FCS_CKM.3 - Cryptographic key access

FCS_CKM.3.1(1) The TSF shall perform the *entry of cryptographic keys* in accordance with a specified cryptographic key access method [*assignment: approved cryptographic key entry method*] that meets the following:

a) manually distributed secret or private cryptographic keys shall be entered into the TOE either by purely manual methods or by electronic methods; and

b) manually entered cryptographic keys or key components shall assure accuracy by having error detection or using duplicate entry; and

c) the entry of secret or private keys shall use split knowledge procedures if unencrypted; and

d) electronically distributed secret or private cryptographic keys shall be entered in encrypted form; and

e) during key entry, keys and key components may be temporarily displayed to allow visual verification and to improve accuracy. When encrypted keys or key components are entered, the resulting plain text secret or private keys shall not be displayed.

Application note: Cryptographic keys should be interpreted as including both seed keys and intermediate keys.

FCS_CKM.3.1(2) The TSF shall perform the *output of cryptographic keys* in accordance with a specified cryptographic key access method [*assignment: approved cryptographic key output method*] that meets the following:

a) manually distributed secret or private cryptographic keys shall be output from the TOE either by purely manual methods or by electronic methods; and

b) the output of secret or private keys shall use split knowledge procedures if unencrypted; and

c) electronically distributed secret or private cryptographic keys shall be output in encrypted form; and

d) all cryptographic keys output for the purposes of archiving shall be encrypted.

5.1.2.4 FCS_CKM.4 - Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*assignment: approved cryptographic key destruction metho*d] that meets the following: *all plain text cryptographic private and secret keys or one time pads should be zeroised.*

5.1.2.5 FCS_COP.1 - Cryptographic operations

FCS_COP.1.1(1) The TSF shall perform *private or authenticated data transfer* in accordance with a specified cryptographic algorithm [*assignment: approved cryptographic algorithm*] and cryptographic key sizes [*assignment: approved cryptographic key size*s] that meet the following: [*assignment: list of approved standard*s].

Application Note: *One of the characteristics of a cryptographic algorithm that influences its cryptographic strength is the size of the keys employed by the algorithm. Many cryptographic algorithms use fixed length keys, and when this is the case, assessment of the cryptographic strength may be straightforward. However, there is a class of cryptographic algorithms that have the capability to vary the key size. For any variable key length algorithms employed within postage meters, the key lengths that are used must be specified in accompanying documentation. As a general guideline, those key lengths should equal or exceed standard current sizes used in comparable revenue-sensitive cryptographic applications.*

For cryptographic algorithms that rely on elliptic curves, only approved elliptic curves which avoid weak elliptic curves should be used.

When a cryptographic algorithm is employed as a data authentication mechanism, the strength of the overall process is directly related to the size of the final authentication code or digital signature that is used. Specific implementations that do not use a long enough authentication code/signature, can severely weaken the authentication technique employed even though the algorithm itself is strong. For any authentication techniques employed within postage meters, the authentication code/signature lengths that are used must be specified in accompanying documentation. As a general guideline, those lengths should equal or exceed standard current sizes used in comparable revenue-sensitive cryptographic authentication applications.

5.1.3 FDP - User Data Protection

5.1.3.1 FDP_ACC.1 - Access control policy

FDP_ACC.1.1 The TSF shall enforce the *Postal Meter Service access control policy* on *requests for the provision of the postal services of a meter by any subject.*

Application note: *The 'objects' of this policy are the postal services of a meter which may be purchased, and the operations covered are requests for the use of a service. The subjects covered are any subject which may request to use such a service.*

5.1.3.2 FDP_ACF.1 - Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce *the Postal Meter Service access control policy* to objects based on *the values of the Cumulative Register and the Remaining Credit Register of the Accounting register, and the value of a transaction for the purchase of postal services of a meter.*

Application note: *This SFR states that the security attributes used to govern the decision as to whether the requested service should be provided are the amount to be paid for the service (an attribute of the 'object') and the values in the accounting register of the postal meter (i.e. there are no 'subject attributes' as such).*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a postal service of a meter may be provided only if:

a) the value of the transaction which is the subject of the operation has not previously been accounted for; and

b) after the operation the notional value of the postage value that has been purchased but remains unused (which is determined by the value of the remaining credit register less the value of the transaction with possible reference to the value of the cumulative register):

- *is greater than or equal to zero ; and*
- *does not exceed its permitted limits.*

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [*assignment: rules, based on security attributes, that explicitly deny provision of a postal service of a meter in addition to the rules specified above*].

5.1.3.3 FDP_DAU.1 - Basic data authentication

FDP_DAU.1.1(1) The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity *of manually entered cryptographic keys or key components*.

FDP_DAU.1.2(1) The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

FDP_DAU.1.1(2) The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *the association between keys entered into or output from a postage meter and the entities (person, group or process) to which the keys are assigned.*

FDP_DAU.1.2(2) The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

5.1.3.4 FDP_IFC.1 - Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the *Revenue-sensitive Module Interface information flow control policy* on *input and output interfaces, data, and operations which cause data to be transferred via input and output interfaces*.

Application note: *The 'subjects' of this policy are in fact the entities attempting to use the interfaces of the revenue-sensitive module, through which information may flow.*

5.1.3.5 FDP_IFF.1 - Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *Revenue-sensitive Module Interface information flow control policy* based on the following types of subject and information security attributes:

a) *type of interface (input or output);*

b) *type of data and encrypted status.*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) *data may be output via any output interface through which plain text cryptographic keys or other critical security parameters could be output only if two independent internal actions are performed first;*

b) *"secret" critical security parameters may be transferred via data input and output ports only if they are in an encrypted form.*

Application note: *Secret critical parameters include intermediate key generation states and values, if the TOE provides a key generation function.*

FDP_IFF.1.3 The TSF shall enforce *no additional information flow control SFP* rules.

Application note: *The SFR has been refined by deletion of the word 'the' for clarity.*

FDP_IFF.1.4 The TSF shall provide *no following additional SFP capabilities.*

Application note: *The SFR has been refined by deletion of the words 'the following' for clarity.*

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: *none.*

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: *all data output via the data output interface shall be inhibited whenever an error state exists and during self-tests.*

5.1.3.6 FDP_ITT.1 - Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the *Postal Meter Service access control policy* to prevent the *modification* of **revenue-sensitive** data when it is transmitted **for printing**.

Application Note: *This requirement shall apply to any meter or revenue-sensitive module which uses physical protection or information (e.g. a digital signature, or cryptography) to guarantee the authenticity of the printed output.*

5.1.3.7 FDP_ITT.3 - Integrity monitoring

FDP_ITT.3.1 The TSF shall enforce the *Postal Meter Service access control policy* to monitor **revenue-related printing operations** for the following errors: *anomalies (i.e. failure or interference) which may result in loss of revenue*.

FDP_ITT.3.2 Upon detection of a **revenue** integrity error, the TSF shall *respond to avoid potential loss of revenue.*

5.1.3.8 FDP_RIP.1 - Residual information protection

FDP_RIP.1.1(1) The TSF shall ensure that any **resource containing accessible secret critical security parameters is zeroised** upon **the allocation of that resource to any subject entering the maintenance role.**

FDP_RIP.1.1(2) The TSF shall ensure that any **resource containing maintenance keys and other secret critical security parameters** is cleared **upon the de-allocation of that resource from a subject exiting the maintenance role.**

5.1.4 FIA - Identification and authentication

5.1.4.1 FIA_UAU.2 - User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.2 FIA_UAU.6 - Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions:

a) when a module is powered up after being powered off (e.g. power failure); or

b) after repair or servicing; or

c) when a module must be returned to a user/crypto service state after entering a safety state; or

d) when a manually distributed secret or private key is entered or output under split knowledge procedures, and if thus configured, the meter shall separately authenticate the operator for each key component.

5.1.4.3 FIA_UID.2 - User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 FMT - Security Management

5.1.5.1 FMT_MOF.1 - Management of functions in TSF

FMT_MOF.1.1 The TSF shall restrict the ability to *enable* the functions *available through the maintenance access interface* to *the authorised maintenance roles*.

5.1.5.2 FMT_MSA.1 - Management of security attributes

FMT_MSA.1.1(1) The TSF shall enforce the *Postal Meter Service access control policy* to restrict the ability to *modify* the *values of the Cumulative and Remaining Credit Registers, and of the services that may be purchased* to *the Revenue Officer*.

Application note: *The SFR has been refined by deletion of the words 'security attributes' for clarity.*

5.1.5.3 FMT_MSA.2 - Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.5.4 FMT_MSA_3 - Static attribute initialisation

FMT_MSA.3.1(1) The TSF shall enforce the *Postal Meter Service access control policy* to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the *Revenue Officer* to specify alternative initial values to override the default values when an object or information is created.

5.1.5.5 FMT_MTD.1 - Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify or substitute* the *secret critical security parameters* to [*assignment: identified roles authorised to access secret critical security parameters*].

FMT_MTD.1.1(2) The TSF shall restrict the ability to *modify or substitute* the *public keys and other authenticated information* to [*assignment: identified roles authorised to access public keys and other authenticated information*].

Application note: *'Other authenticated information' comprises any information whose authenticity is a requirement or objective of the meter's operation or security (e.g. register values, digital signatures, etc.).*

FMT_MTD.1.1(3) The TSF shall restrict the ability to *zeroise un-encrypted critical security parameters* to *a specified set of operators*.

5.1.5.6 FMT_SMR.1 - Security management roles

FMT_SMR.2.1 The TSF shall maintain the roles

a) User role; and

b) Maintenance role; and

c) *Revenue-officer role.*

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the *following conditions for the different role*s are satisfied:

a) *the operator explicitly or implicitly selects one or more roles; and*

b) *the authorisation of the operator to assume a previously un-authenticated role shall be authenticated; and*

c) *for identity-based authentication, the operator may not adopt two or more roles simultaneously.*

Application note: *The SFR has been refined for clarity by appending the list of specified conditions.*

5.1.6 FPT - Protection of the TOE Security Functions

5.1.6.1 FPT_AMT.1 - Underlying abstract machine test

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up and [assignment: other conditions approved by the postal authorities]* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF

5.1.6.2 FPT_FLS.1 - Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*assignment: known errors resulting in an error state as specified by the ST author*].

5.1.6.3 FPT_PHP.1 - Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical **probing of the revenue-sensitive modules via any ventilation openings** that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical **probing of the revenue-sensitive modules via any ventilation openings** has occurred.

5.1.6.4 FPT_PHP.3 - Resistance to physical attack

FPT_PHP.3.1(1) The TSF shall resist *physical tampering* to the *chips in revenue-sensitive modules* by responding automatically such that the TSP is not violated.

Refinement: **The chips shall be of production quality that shall include standard passivation techniques.**

FPT_PHP.3.1(2) The TSF shall resist *physical tampering* to *revenue-sensitive modules* by responding automatically such that the TSP is not violated.

Refinement: **Automatic response by the TSF shall take the following form:**

a) Single-chip revenue-sensitive modules shall be enclosed in a hard, opaque, removal-resistant coating.

b) Multiple-chip embedded and multiple-chip standalone revenue-sensitive modules shall be enclosed:

- **within in a hard opaque potting material; or**
- **within a strong non-removable enclosure; or**
- **within a strong removable cover, and with tamper-response and zeroisation circuitry.**

so that the module is rendered inoperable and/or the secret critical revenue sensitive data is zeroised as appropriate.

FPT_PHP.3.1(3) The TSF shall resist *the following environmental conditions or fluctuations outside the normal operating range of the revenue-sensitive module:*

- *high positive voltage;*
- *high negative voltage;*
- *high temperature;*
- *low temperature;*
- *short exposure to common chemicals;*
- *long exposure to common contaminants;*
- *vibration;*
- *shock;*
- *physical interference;*
- *printer endurance;*
- *electromagnetic radiation (e.g. X rays, ultra-violet light and microwaves);*
- *low air pressure;*
- *high humidity;*
- *rapid changes in the environment (temperature, pressure and humidity);*
- *frequent changes in the environment (temperature, pressure and humidity);*
- *EMI/EMC (beyond common national standards).*

by responding automatically such that the TSP is not violated.

Refinement: **Either EFP or EFT features shall be used for each identified condition. If EFP is chosen for a particular condition – the revenue-sensitive module shall monitor and correctly respond to fluctuations in the condition, as appropriate, outside of the module's specified normal operating range for that condition. The protection feature shall involve additional electronic circuitry or devices that shall continuously measure these environmental conditions. If a condition is determined to be outside of the module's normal operating range, the protection circuitry shall either:**

- **shut down the revenue-sensitive module; or**
- **immediately actively zeroise all unprotected critical security parameters within the module.**

5.1.6.5 FPT_RCV.1 - Manual recovery

FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

Refinement: **After a soft error that is one not requiring maintenance, service or repair, the TSF shall enter an error state where the ability to return the TOE to an acceptable operational or initialisation state is provided.**

5.1.6.6 FPT_RVM.1 - Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Refinement: **All information flow and physical access to the module shall be restricted to logical interfaces that define all entry points to and from the module, and which are logically distinct from each other.**

5.1.6.7 FPT_SEP.1 - Domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.8 FPT_STM.1 - Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.6.9 FPT_TST.1 - TSF testing

FPT_TST.1.1 The TSF shall run a suite of tests *during initial start-up and [assignment: other conditions approved by the postal authorities*] to demonstrate the correct operation of the TSF.

Application Note *The tests shall include tests to output the current status for a module.*

Typical of power up tests are: cryptographic algorithm tests, software/firmware tests, critical functions tests, and statistical random number generator tests.

Typical of conditional tests are: pair-wise consistency tests for public and private keys, software/firmware load tests, manual entry test of critical security parameters, continuous random number generator tests

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.7 FTP - Trusted path/channels

5.1.7.1 FTP_TRP.1 - Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***operators*** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

Refinement: **The trusted path shall be logically disconnected from the circuitry and processes performing key generation, manual key entry, or key zeroisation.**

FTP_TRP.1.2 The TSF shall permit *the TSF or* ***operators*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *the input and output of cryptographic key components,* [assignment: *other services for which trusted path is required*].

5.2 TOE Security Assurance Requirements

The target evaluation assurance level for the product is EAL4 augmented (see [CC3] for a definition of EAL4). Additionally, certain assurance requirements elements are refined. For clarity, therefore, the assurance requirements are stated in full below.

CLASS	FAMILY	COMPONENT	REFINED?
ACM	ACM_AUT	ACM_AUT.1	
	ACM_CAP	ACM_CAP.4	Y
	ACM_SCP	ACM_SCP.2	
ADO	ADO_DEL	ADO_DEL.2	
	ADO_IGS	ADO_IGS.1	
ADV	ADV_FSP	ADV_FSP.3	Y
	ADV_HLD	ADV_HLD.3	Y
	ADV_IMP	ADV_IMP.1	Y
	ADV_LLD	ADV_LLD.1	Y
	ADV_RCR	ADV_RCR.2	
	ADV_SPM	ADV_SPM.1	
AGD	AGD_ADM	AGD_ADM.1	Y
	AGD_USR	AGD_USR.1	
ALC	ALC_DVS	ALC_DVS.1	Y
	ALC_LCD	ALC_LCD.1	
	ALC_TAT	ALC_TAT.1	
ATE	ATE_COV	ATE_COV.2	Y
	ATE_DPT	ATE_DPT.1	
	ATE_FUN	ATE_FUN.1	
	ATE_IND	ATE_IND.2	

CLASS	FAMILY	COMPONENT	REFINED?
AVA	AVA_MSU	AVA_MSU.2	
	AVA_SOF	AVA_SOF.1	
	AVA_VLA	AVA_VLA.3	

Table 2 - Security Assurance Requirements for the model

5.2.1 ACM - Configuration Management

5.2.1.1 ACM_AUT.1 - Partial CM automation

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

ACM_AUT.1.2D The developer shall provide a CM plan.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Evaluator action elements:

ACM_AUT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.2 ACM_CAP.4 - Generation support and acceptance procedures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

Refinement: **The CM system shall uniquely identify all the individual hardware and software components of the revenue-sensitive modules identified by the vendor in agreement with the postal authorities.**

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.1.3 ACM_SCP.2 - Problem tracking CM coverage

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 ADO - Delivery and Operation

5.2.2.1 ADO_DEL.2 - Detection of modification

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 ADO_IGS.1 - Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 ADV - Development

5.2.3.1 ADV_FSP.3 - Semiformal functional specification

Developer action elements:

ADV_FSP.3.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.3.1C The functional specification shall describe the TSF and its external interfaces using a semiformal style, supported by informal, explanatory text where appropriate.

ADV_FSP.3.2C The functional specification shall be internally consistent.

ADV_FSP.3.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

Refinement: **The functional specification shall define and specify all physical and logical input and output data paths within the module.**

ADV_FSP.3.4C The functional specification shall completely represent the TSF.

Refinement: **The module shall have at least the following four logical interfaces:**

- **data input interface;**
- **data output interface;**
- **control input interface;**
- **status output interface.**

Application note: *The module may also include the following logical interfaces:*

- *power interface;*
- *maintenance access interface.*

ADV_FSP.3.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 ADV_HLD.3 - Semiformal high-level design

Developer action elements:

ADV_HLD.3.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.3.1C The presentation of the high-level design shall be semiformal.

Refinement: **The high-level design shall describe all states of each revenue-sensitive module including the following:**

a) All of the state transitions of each module shall be described.

b) The states shall be described using finite state diagrams of sufficient detail.

c) The following states shall be described for all revenue-sensitive modules:

- **the power on/off states;**
- **the Revenue-officer states;**
- **the critical security parameter entry states;**
- **the user service states;**
- **the self test states; and**
- **the error states.**

d) For all revenue-sensitive modules which include a maintenance access interface, its maintenance states shall be described.

ADV_HLD.3.2C The high-level design shall be internally consistent.

ADV_HLD.3.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

Refinement: **The high-level design shall:**

a) include a block diagram depicting all major hardware components of the module and their interconnections;

b) include for each sub-system the service, the service inputs, corresponding service outputs, and the authorised role or set of roles in which the service can be performed.

ADV_HLD.3.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.3.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.3.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.3.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.3.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of all effects, exceptions and error messages.

ADV_HLD.3.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Refinement: **The description of separation in the high-level design shall:**

a) completely specify the module's revenue-sensitive boundary surrounding the components.

b) explain why any non-TSP enforcing subsystems do not affect the security of the module.

Evaluator action elements:

ADV_HLD.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.3.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 ADV_IMP.1 - Subset of the implementation of the TSF

Developer action elements:

ADV_IMP.1.1D The developer shall provide the implementation representation for a selected subset of the TSF.

Content and presentation of evidence elements:

ADV_IMP.1.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

Refinement: **Source code shall comply with the following:**

a) For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software.

b) All software within a revenue-sensitive module shall be implemented using a high-level language, except that the limited use of low-level languages (e.g., assembly languages) is allowed when it is essential to the performance of the module or when a high-level language is not available.

ADV_IMP.1.2C The implementation representation shall be internally consistent.

Evaluator action elements:

ADV_IMP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.1.2E The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.4 ADV_LLD.1 - Descriptive low-level design

Developer action elements:

ADV_LLD.1.1D The developer shall provide the low-level design of the TSF.

Content and presentation of evidence elements:

ADV_LLD.1.1C The presentation of the low-level design shall be informal.

ADV_LLD.1.2C The low-level design shall be internally consistent.

ADV_LLD.1.3C The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

Refinement: **The description of separation in the low-level design shall:**

a) completely specify the module's revenue-sensitive boundary surrounding the components.

b) explain why any non-TSP enforcing components do not affect the security of the module.

Evaluator action elements:

ADV_LLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_LLD.1.2E The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.5 ADV_RCR.2 - Semiformal correspondence demonstration

Developer action elements:

ADV_RCR.2.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.2.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.2.1C For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

Evaluator action elements:

ADV_RCR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.6 ADV_SPM.1 - Informal TOE security policy model

Developer action elements:

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 AGD - Guidance documents

5.2.4.1 AGD_ADM.1 - Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

Refinement: **The administrator guidance shall describe completely all of the authorised roles supported by the module.**

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 AGD_USR.1 - User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 ALC - Life-cycle support

5.2.5.1 ALC_DVS.1 - Identification of security measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

Refinement **In particular, the development security documentation will describe the security measures for initialising the access control mechanisms of the modules.**

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.5.2 ALC_LCD.1 - Developer defined life-cycle model

Developer action elements:

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

Content and presentation of evidence elements:

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

Evaluator action elements:

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.3 ALC_TAT.1 - Well-defined development tools

Developer action elements:

ALC_TAT.1.1D The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D The developer shall document the selected implementation-dependent options of the development tools.

Content and presentation of evidence elements:

ALC_TAT.1.1C All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

Evaluator action elements:

ALC_TAT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 ATE - Tests

5.2.6.1 ATE_COV.2 - Analysis of coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Refinement **The analysis of the test coverage shall demonstrate that EFT tests are identified in the test documentation that confirm the revenue sensitive modules will not be affected by environmental conditions or fluctuations outside of the module's normal operating range in a manner that can**

compromise the security of the module for those conditions or fluctuations not covered by EFP.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.2 ATE_DPT.1 - Testing: high-level design

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.3 ATE_FUN.1 - Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6.4 ATE_IND.2 - Independent testing – sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.2.7 AVA - Vulnerability assessment

5.2.7.1 AVA_MSU.2 - Validation of analysis

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.

AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C The analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4E The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.2.7.2 AVA_SOF.1 - Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Application note: *This includes any random number generator used in the key generation process.*

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.2.7.3 AVA_VLA.3 - Moderately resistant

Developer action elements:

AVA_VLA.3.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.3.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.3.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.3C The evidence shall show that the search for vulnerabilities is systematic**.**

Evaluator action elements:

AVA_VLA.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.3.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.3.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.3.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.3.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.

5.3 Strength of Function

The claimed strength of function is *SOF-medium*.

The strength of cryptographic algorithms is outside the scope of the CC, and hence the assessment of algorithmic strength will not form part of the TOE evaluation.

5.4 Security Requirements for the IT Environment

The following SFR is a requirement for the IT environment since it is needed to satisfy other FCS dependencies, and to satisfy OE.Key_Gen. [IPMAR] identifies this as an ‘optional’ requirement on the TOE in that it must be satisfied *only* if the TOE provides a key generation function.

All other objectives are procedural and hence do not give rise to security requirements on the IT environment.

5.4.1.1 FCS_CKM.1 - Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: approved cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: approved cryptographic key sizes*] that meet the following: [*assignment: list of approved standards*].

6. OPERATING SYSTEM FUNCTIONAL PACKAGE

The PP requirements should be augmented with the SFRs defined in the following functional package if the TOE provides a means whereby an operator can load or execute software or firmware that is not part of the TOE. These SFRs are needed to achieve the TOE security objective O.Label, and also to ensure that O.Access and O.Integrity are upheld, as well as O.Crypto.

Note that iteration numbers are continued from the sequences in section 5. The identified iteration numbers in the table below indicate the *total* number of iterations of that component when the core requirements are taken into account.

CLASS	FAMILY	COMPONENT	REFINED?
FCS	FCS_COP	FCS_COP.1 (*2)	
FDP	FDP_DAU	FDP_DAU.1 (*3)	
	FDP_ETC	FDP_ETC.1	Y
	FDP_IFC	FDP_IFC.1 (*2)	
	FDP_IFF	FDP_IFF.2	Y
	FDP_ITC	FDP_ITC.1	Y
FMT	FMT_MSA	FMT_MSA.1 (*3)	
	FMT_MSA	FMT_MSA.3 (*2)	
	FMT_MTD	FMT_MTD.1 (*9)	Y

Table 3 - Security Functional Requirements in the Functional Package

6.1.1 FCS - Cryptographic Services

6.1.1.1 FCS_COP.1 - Cryptographic operations

FCS_COP.1.1(2) The TSF shall perform [*assignment: cryptographic mechanism to authenticate revenue-sensitive software*] in accordance with a specified cryptographic algorithm [*assignment: approved cryptographic algorith*m] and cryptographic key sizes [*assignment: approved cryptographic key size*s] that meet the following: [*assignment: list of approved standard*s].

Application note: *This SFR relates to specifically to FDP_DAU.1(3). The first assignment is partially completed - the ST author should specify the mechanism used (e.g. data authentication code, digital signature).*

6.1.2 FDP - User Data Protection

6.1.2.1 FDP_DAU.1 - Basic data authentication

FDP_DAU.1.1(3) The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *the revenue-sensitive software within the revenue-sensitive module.*

FDP_DAU.1.2(3) The TSF shall provide [assignment: *list of subject*s] with the ability to verify evidence of the validity of the indicated information.

Application note: *The assignment operation is left for the ST author to complete by specifying who can authenticate the revenue-sensitive software. The method of authentication may be, for example, by data authentication code or digital signature. FDP_DAU.2 may be included in the ST to specify the use of digital signatures; as this is hierarchic to FDP_DAU.1, the PP requirements will be satisfied.*

6.1.2.2 FDP_ETC.1 - Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the *Mandatory Access Control* Policy when exporting user data, controlled under the **MAC policy**, outside the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.2.3 FDP_IFC.1 - Subset information flow control

FDP_IFC.1.1(2) The TSF shall enforce the *Mandatory Access Control policy* on *subjects; revenue-sensitive software, critical security parameters, control and status information, and all operations among subjects and objects covered by the MAC policy*.

6.1.2.4 FDP_IFF.2 - Hierarchical security attributes

FDP_IFF.2.1 The TSF shall enforce the *Mandatory Access Control policy* based on the following types of subject and information security attributes:

a) The sensitivity label of the subject; and

b) The sensitivity label of the object containing the information.

FDP_IFF.2.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules, based on the ordering relationships between security attributes hold:

a) If the sensitivity label of the subject is greater than or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);

b) If the sensitivity label of the object is greater than or equal to the sensitivity label of the subject; then the flow of information from the subject to the object is permitted (a write operation);

*c) If the sensitivity label of subject **A** is greater than or equal to the sensitivity label of subject B; then the flow of information from subject **B** to subject **A** is permitted.*

FDP_IFF.2.3 The TSF shall enforce *no additional information flow control SFP rules*.

Application note: The SFR has been refined by deletion of the word 'the' for clarity.

FDP_IFF.2.4 The TSF shall provide *no additional SFP capabilities*.

Application note: The SFR has been refined by deletion of the words 'the following' for clarity.

FDP_IFF.2.5 The TSF shall explicitly authorise an information flow based on the following rules: *none*.

FDP_IFF.2.6 The TSF shall explicitly deny an information flow based on the following rules: *none.*

FDP_IFF.2.7 The TSF shall enforce the following relationships for any two valid **sensitivity labels**:

a) There exists an ordering function that, given two valid **sensitivity labels**, determines if the **sensitivity labels** are equal, if one **sensitivity label** is greater than the other, or if the **sensitivity labels** are incomparable; and

b) There exists a "least upper bound" in the set of **sensitivity labels**, such that, given any two valid **sensitivity labels**, there is a valid **sensitivity label** that is greater than or equal to the two valid **sensitivity labels**; and

c) There exists a "greatest lower bound" in the set of the **sensitivity labels**, such that, given any two valid **sensitivity labels**, there is a valid **sensitivity label** that is not greater than the two valid **sensitivity labels**.

6.1.2.5 FDP_ITC.1 - Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the *Mandatory Access Control policy* when importing user data, controlled under the **MAC policy**, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the **MAC policy** from outside the TSC: [assignment: *additional importation control rules*].

6.1.3 FMT - Security Management

6.1.3.1 FMT_MSA.1 - Management of security attributes

FMT_MSA.1.1(2) The TSF shall enforce the *Mandatory Access Control policy* to restrict the ability to *modify* the *object labels* to *the Revenue Officer*.

FMT_MSA.1.1(3) The TSF shall enforce the *Mandatory Access Control policy* to restrict the ability to *modify* the *clearance of operators* to *the Revenue Officer*.

6.1.3.2 FMT_MSA_3 - Static attribute initialisation

FMT_MSA.3.1(2) The TSF shall enforce the *Mandatory Access Control policy* to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the *Revenue Officer* to specify alternative initial values to override the default values when an object or information is created.

6.1.3.3 FMT_MTD.1 - Management of TSF data

FMT_MTD.1.1(4) The TSF shall restrict the ability to *execute* the *cryptographic program images contained on the revenue-sensitive module's secondary storage* to a *specified set of operators*.

FMT_MTD.1.1(5) The TSF shall restrict the ability to *modify, replace or delete* the *entities within the following components* to *a specified set of operators*:

- *cryptographic programme images on secondary storage;*
- *cryptographic data (e.g. cryptographic keys, audit data) stored on secondary storage;*
- *cryptographic data (e.g. cryptographic keys, audit data) stored in computer memory;*
- *other critical security parameters stored on secondary storage;*
- *other critical security parameters contained in computer memory.*

FMT_MTD.1.1(6) The TSF shall **prevent attempts** to *modify* the *loaded and executing cryptographic programme images* **by** *any operator or executing process*.

Application note *Executing processes, in this case, means all non-operating system (i.e., all operator initiated) processes, cryptographic or not.*

This SFR has been refined for clarity, replacing 'restrict the ability' with 'prevent attempts' and the final 'to' with 'by'. This SFR is equivalent to completing the unrefined requirements element in such a way as to restrict the ability to modify the program images to the empty set of operators and executing processes.

FMT_MTD.1.1(7) The TSF shall restrict the ability to *read* the *entities within the following components* to *specified distinct sets of operators:*

- *cryptographic data (e.g. cryptographic keys, audit data) stored on secondary storage;*
- *cryptographic data (e.g. cryptographic keys, audit data) stored in computer memory;*
- *other critical security parameters stored on secondary storage;*
- *other critical security parameters contained in computer memory;*
- *plain text data stored either within the meter's memory or on secondary storage.*

FMT_MTD.1.1(8) The TSF shall **prevent attempts** to *read* the *following revenue-sensitive module software components* **by** *any operator or executing process*:

- *cryptographic programme images contained on secondary storage;*
- *executing cryptographic programme images.*

Application note: *This SFR has been refined for clarity, replacing 'restrict the ability' with 'prevent attempts' and the final 'to' with 'by'. This SFR is equivalent to completing the unrefined requirements element in such a way as to restrict the ability to read the software components to the empty set of operators and executing processes.*

FMT_MTD.1.1(9) The TSF shall restrict the ability to *enter* the *cryptographic keys and other critical security parameters* to *a specified set of operators*.

A PP RATIONALE

This annex demonstrates the suitability of the choice of security objectives, security requirements and TOE summary specification aspects.

A.1 Security Objectives Rationale

This section demonstrates how the threats, organisational security policies and assumptions are met by the security objectives. The correlation between the security needs and the objectives is given in table 4, below.

Objectives:	O.Access	O.Audit	O.Crypto	O.Enforcement	O.Failsafe	O.IA	O.Integrity	O.Manage_Maintenance	O.Manage_Revenue	O.Label	O.Path	O.Probe	O.Stress	O.Tamper	OE.Admin	OE.Audit	OE.Em	OE.Key_Generation	OE.IA	OE.Postal_Authority
Threats																				
T.Access	x	x	x	x		x		x	x	x	x				x	x	x	x	x	
T.Authority		x		x		x										x			x	
T.Counterfeit			x															x		
T.Integrity		x	x	x		x	x									x		x	x	
T.Masquerade		x	x	x												x		x		x
T.Non_Secure		x			x											x				
T.Postal_Authority_Access	x	x	x	x												x		x		x
T.Probe								x				x								
T.Role	x	x		x		x		x	x						x	x				
T.Stress													x							
T.Tamper								x						x						
Policies																				
P.Accountable		x				x										x			x	
P.Access	x																			
P.Crypto			x															x		
Assumptions																				
A.Em																	x			
A.No_Evil															x					

Table 4 - Correlation between the Security Needs and Objectives

A.1.1 Security objectives suitable to counter the threats

The following rationale demonstrates how the objectives counter the threats:

[T.Access] *An attacker may try to gain access to services or information protected by the TOE for which he is not authorised.*

This threat is mainly countered by O.Access which provides the means for controlling and limiting access of users and their subjects to those objects and resources for which they are responsible. O.Label provides support in the event that the TOE provides the means by which an operator can load and execute software or firmware that is not part of the TOE.

O.Crypto with OE.Key_Generation supports O.Access by securing cryptographic key material through the key life-cycle - that is generation, distribution, access, and destruction in a secure manner.

O.Manage_Maintenance limits the access to maintenance services of the TOE to authorised maintenance operators. O.Manage_Revenue limits the access to the revenue sensitive and cryptographic services of the TOE to revenue officers.

O.Path provides a secure path to the TSF thus preventing attackers gaining access to services or information of the TOE by compromising the communications path between operators and TSF of the TOE.

O.Audit and OE.Audit support O.Access by recording security relevant events which might leave the TOE access policies of the TOE mis-configured, and by noting potential or real violations of the access policies.

O.Enforcement supports O.Access by ensuring the security policies of the TSF are not bypassed in particular those relating to securing access.

O.IA together with OE.IA supports O.Access by ensuring that only bone-fide operators gain access to the TOE and providing the mechanism to limit access to the resources of the TOE to users acting within particular roles.

OE.Admin ensures that revenue officers are suitably vetted, and thus do not act collectively to compromise information known only to the postal authorities.

OE_Em ensures that attackers do not gain access to information from electromagnetic emissions or emanations from the TOE.

[T.Authority] *An attacker may try to impersonate an authorised user (or operational group) of the TOE thereby gaining unauthorised access to the TOE and thus to information or services of the TOE.*

O.IA together with OE.IA compels operators of the TOE to authenticate to the TOE and to the role in which they intend to use the TOE.

O.Enforcement supports O.IA by ensuring the security policies of the TSF are not bypassed in particular those relating to authentication.

O.Audit with OE.Audit supports O.IA by recording security relevant events which might leave authentication policies of the TOE mis-configured, and by noting potential or real violations of the authentication policies.

[T.Counterfeit] *An attacker may be able to gain access to the postal services of the TOE by counterfeiting postal indicia.*

O.Crypto with OE_Key_Generation provides cryptographic support enabling postal indicia to embed cryptographic signatures which may be used to authenticate the originating postal meter.

[T.Integrity] *An attacker may try to modify services or information protected by the TOE for which he is not authorised.*

O.Integrity provides the main functionality to counter this threat by detecting the loss of integrity of critical data and revenue sensitive software images.

O.Crypto with OE_Key_Generation provides the capability to authenticate information and the loadable images of service software of the TOE.

O.Enforcement ensures that the security policies in particular ensuring the integrity of secured information and software is enforced.

O.Audit with OE.Audit supports detection of any security related events that might compromise the integrity of the TOE.

O.IA with OE.IA supports O.Integrity by ensuring that only bone-fide operators gain access to the TOE and providing the mechanism to limit access to the resources of the TOE to users acting within particular roles.

[T.Masquerade] *An attacker gains access to services or information protected by the TOE by masquerading as a postal authority.*

OE_Postal_Authority ensures that the postal authorities maintain the security of their cryptographic keys so attackers cannot pretend to be a postal authority using the postal authority's authentic keys. This objective also ensures that the postal meter has authentic certificates from the postal authorities so that the meter is able to authenticate the origin of communications purporting to be from a postal authority.

O.Crypto with OE_Key_Generation supports cryptographic operations in a secure manner in particular allowing the authentication of communications purporting to be from a postal authority.

O.Audit with OE.Audit supports these other objectives by providing the means to detect untoward cryptographic events which might lead to a compromise.

O.Enforcement ensures that the security policies in particular ensuring the security of cryptographic operations and key life-cycle are enforced.

[T.Non_Secure] *An attacker may try to force the TOE into a non-secure state by causing the TOE to error or reset.*

O.Failsafe counters the threat by preserving a secure state in the event of error or reset.

O.Audit with OE.Audit supports the primary objective by providing the means to detect security events in particular error and reset states.

[T.Postal_Authority_Access]

An attacker may try to access information protected by the TOE which is reserved exclusively to a postal authority.

O.Access provides the means for controlling and limiting access of users and their subjects to those objects and resources for which they are responsible.

O.Audit with OE.Audit supports this objective by detecting security relevant events.

OE_Postal_Authority ensures that the postal authorities maintain the security of their cryptographic keys so attackers cannot pretend to be a postal authority using the postal authority's authentic keys.

O.Crypto with OE_Key_Generation supports O.Access by supporting the cryptographic functions in a secure manner.

O.Enforcement supports these objects by ensuring that the relevant policies are enforced.

[T.Probe] *An attacker may try to perform passive probing of the TOE to reveal design or operational content.*

O.Probe counters the threat by protecting the TOE and its assets from physical probing.

O.Manage_Maintenance supports this objective by ensuring that only authorised maintenance officers are able to access maintenance functionality.

[T.Role] *An authorised user of the TOE may try to access information or services protected by the TOE which are reserved to another authorised role for which he has no authorisation.*

O.Access counters the threat by controlling and limiting access on the basis of the TOE's access control policies.

O.IA supports this objective by ensuring operators of the TOE are authenticated in their roles.

O.Manage_Maintenance and O.Manage_Revenue help counter the threat by ensuring that only maintenance officers and revenue officers have access to the functionality needed in the performance of their respective roles.

O.Audit with OE.Audit supports these objectives by providing the means to detect security events in particular the unauthorised use of information or services of another role.

O.Enforcement ensures that the security policies in particular those ensuring authorised access to information and services are enforced.

OE.Admin ensures that revenue officers are suitably vetted, and thus do not act collectively to compromise information known only to the postal authorities.

[T.Stress] *An attacker may try to gain or modify information protected by the TOE for which he is not authorised by subjecting it to environmental stress.*

O.Stress counters the threat by protecting the TOE and its assets from environmental stress including electrical, electronic and electromagnetic stress.

[T.Tamper] *An attacker may try to actively interfere with the TOE to cause the TOE to perform outside of its design or to reveal operational content.*

O.Tamper counters the threat by protecting the TOE and its assets from unauthorised physical tampering.

O.Manage_Maintenance helps support this objective by ensuring only authorised maintenance officers have access to the maintenance functionality of the TOE.

A.1.2 Security objectives suitable to meet OSPs

The following rationale demonstrates how the objectives achieve the OSPs:

[P.Accountable] *The users of the system shall be held accountable for their actions within the system.*

O.IA with OE.IA ensures that operators of the TOE are identified by the TOE either individually or else within some role.

OE.Audit with O.Audit ensures that actions against the security of the system are detected so that operators may be held accountable.

[P.Access] *The right to access postal services of the postal meter shall be determined by the Postal Meter Service access control policy based on:*

- *the value of the cumulative register; and*
- *the value of the remaining credit register; and*
- *the value(cost) of the requested service*.

The right to postal services shall depend on whether there are sufficient funds remaining to pay for the requested service.

O.Access ensures that access to information and services is limited to authorised users in accordance with the access control policies, in particular the Postal Meter Service access control policy.

[P.Crypto] *The cryptographic key management, key operations and algorithms used by the TOE shall comply with standards approved by the postal authorities.*

O.Crypto and OE_Key_Generation ensures that the TOE supports cryptographic functions securely and in accordance with the rules defined by P.Crypto.

A.1.3 Security objectives suitable to uphold assumptions

The following rationale demonstrates how the objectives cover the assumptions:

[A.Em] It is assumed that appropriate consideration shall have been given to the design issues associated with EMI/EMC within the meter, in particular the EMI/EMC of the meter shall comply with the national legislation for such meters.

OE.Em upholds this assumption.

[A.No_Evil] It is assumed that there are one or more individuals who are assigned to administer the TOE. These individuals are not collectively careless, wilfully negligent or hostile.

OE.Admin upholds this assumption.

A.2 Security Requirements Rationale

A.2.1 Security Functional Requirements suitable to achieve the security objectives

This section provides the correlation and justification of suitability between the objectives and the Security Functional Requirements. Iteration numbers of components are given where appropriate - if no iteration number is given then **all** iterations of that component help to achieve the security objective (including, where relevant, those in the *Operating system functional package*).

Security Objectives to be met by the TOE	Security Functional Requirement
O.Access	Access control policy FDP_ACC.1 Access control functions FDP_ACF.1 Subset information flow control FDP_IFC.1(1) Simple security attributes FDP_IFF.1 Residual Information Protection FDP_RIP.1 Management of TSF data FMT_MTD.1
O.Audit	Security audit data generation FAU_GEN.1 Reliable time stamps FPT_STM.1
O.Crypto	Cryptographic key distribution FCS_CKM.2 Cryptographic key access FCS_CKM.3 Cryptographic key destruction FCS_CKM.4 Cryptographic operations FCS_COP.1
O.Enforcement	Non-bypassability of the TSP FPT_RVM.1 Domain separation FPT_SEP.1 Underlying abstract machine test FPT_AMT.1 TSF Testing FPT_TST.1
O.Failsafe	Failure with preservation of secure state FPT_FLS.1 Manual recovery FPT_RCV.1

Security Objectives to be met by the TOE	Security Functional Requirement
O.IA	User authentication before any action FIA_UAU.2 Re-authenticating FIA_UAU.6 User identification before any action FIA_UID.2 Security Management Roles FMT_SMR.2
O.Integrity	Basic internal transfer protection FDP_ITT.1 Integrity monitoring FDP_ITT.3 Basic data authentication FDP_DAU.1
O.Manage_Maintenance	Management of functions in TSF FMT_MOF.1 Secure security attributes FMT_MSA.2 Management of TSF data FMT_MTD.1(3) Security Management Roles FMT_SMR.2
O.Manage_Revenue	Management of security attributes FMT_MSA.1(1) Secure security attributes FMT_MSA.2 Static Attribute Initialisation FMT_MSA.3(1) Management of TSF data FMT_MTD.1 Security Management Roles FMT_SMR.2
O.Path	Trusted path/channels FTP_TRP.1
O.Probe	Passive detection of physical attack FPT_PHP.1

Security Objectives to be met by the TOE	Security Functional Requirement
O.Stress	Resistance to physical attack FPT_PHP.3(3)
O.Tamper	Resistance to physical attack FPT_PHP.3(2)
O.Label	Subset information flow control FDP_IFC.1(2) Hierarchical security attributes FDP_IFF.2 Export of user data without security attributes FDP_ETC.1 Import of user data without security attributes FDP_ITC.1 Management of security attributes FMT_MSA.1(2-3) Static Attribute Initialisation FMT_MSA.3(2)

Table 5 - Correlation between Objectives for the TOE and SFRs

O.Access FDP_ACC.1 identifies the access control policies of the TSF. FDP_ACF.1 ensures that the identified access control policies are enforced. FDP_IFC.1(1) identifies the module interface information flow control policies of the TOE and FDP_IFF.1 ensures that the policy is enforced. FDP_RIP.1 ensures that no residual secret security critical data is available on entry to the maintenance role, nor any maintenance security critical data is available to other roles on exit from the maintenance role. Such accesses would be in contravention of the access control and information flow control policies, viz. The provision of postal meter services and information flow via the interfaces of the module. FMT_MTD.1 ensures access to critical security parameters and cryptographic programme images is appropriately controlled.

O.Audit FAU_GEN.1 ensures that audit data is generated for security events identifying, among other things, the operator and date and time. FPT_STM.1 ensures that TSF is able to provide reliable time stamps for the audit records.

O.Crypto FCS_CKM.2 ensures that cryptographic keys are distributed in accordance with a specified method and to given standards FCS_CKM.3 ensures that the entry of keys into the TSF is in accordance with a specified method and to given standards. FCS_CKM.4 ensures that keys are destroyed using

zeroisation. FCS_COP.1 ensures that cryptographic operations are performed with specified methods and to given standards.

O.Enforcement FPT_RVM.1 ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC proceeds. FPT_SEP.1 ensures that the TSF maintains a separate security domain from untrusted processes. FPT_AMT.1 and FPT_TST.1 ensure that the TSF is operating correctly and continues to operate correctly by using a series of tests of the underlying abstract machine and also the operations on this abstract machine.

O.Failsafe FPT_FLS.1 ensures that a secure state is preserved when known errors arise. FPT_RCV.1 ensures that a secure state is preserved when a need for reset arises.

O.IA FIA_UID.2 and FIA_UAU.2 ensure that user is successfully identified and authenticated before allowing other TSF mediated actions to proceed. FIA_UAU.6 ensures that the user is compelled to re-authenticate should certain states arise. FMT_SMR.2 identifies the various roles available at the TOE and ensures users are associated with roles, and ensures that the authorisation of a user to be in a role has been authenticated before allowing the user to proceed in that role.

O.Integrity FDP_ITT.1 enforces the access control policy to prevent any loss in integrity when data is sent for printing. FDP_ITT.3 ensures the TOE responds to revenue sensitive printing anomalies. FDP_DAU.1 provides the capability to detect the loss of integrity of manually entered cryptographic data, and of the integrity of the association between keys and the entity to which they are assigned, and the integrity of revenue sensitive software.

O.Manage_Maintenance
FMT_MOF.1 ensures that only maintenance officers may enable functions available through the maintenance access interface. FMT_MSA.2 ensures that secure values are accepted for security attributes. FMT_MTD.1 ensures that revenue sensitive program images may only be executed by a specified set of operators, and similarly for cryptographic data and program images. FMT_SMR.2 identifies the various roles available at the TOE and ensures users are associated with roles, and ensures that the authorisation of a user to be in a role has been authenticated before allowing them to proceed in that role, in particular the maintenance role.

O.Manage_Revenue
FMT_MSA.1 ensures the revenue officer is able to manage the values of the accounting register and the postal services. FMT_MSA.2 ensures that secure values are accepted for security attributes. FMT_MSA.3 ensures the revenue officer may initialise revenue sensitive security attributes. FMT_MTD.1 ensures that revenue sensitive program images may only be executed by a specified set of operators, and similarly for cryptographic data

and program images. FMT_SMR.2 identifies the various roles available at the TOE and ensures users are associated with roles, and ensures that the authorisation of a user to be in a role has been authenticated before allowing them to proceed in that role, in particular the revenue officer role.

O.Path FTP_TRP.1 ensures that there is a trusted path for secure communication between users and the TSF, and that the user may initiate such communication.

O.Probe FPT_PHP.1 ensures that the TOE detects physical probing that might compromise the TOE.

O.Stress FPT_PHP.3(3) ensures that the TOE resists environmental stressing either by actively zeroising unprotected critical security parameters or shutting down leaving the TOE in a passive but secure state.

O.Tamper FPT_PHP.3(2) ensures that the TOE resists physical tampering either by being physically resistant and/or by actively zeroising unprotected critical parameters.

The following objective is to be met only if the TOE provides operators with the ability to load and execute firmware and software that is not part of the TOE. It is met by SFRs included in the *Operating System functional package*.

O.Label FDP_IFC.1(1) and FDP_IFF.2 ensure that the information to be protected is labelled and access to this information controlled on the basis of these labels and subject clearances. FDP_ITC.1 and FDP_ETC.1 govern, respectively, the import and export of this information. FMT_MSA.3(2) ensures that labels are assigned appropriately on creation of information. FMT_MSA.1(2) and FMT_MSA.1(3) ensure that only the revenue officer may modify sensitivity labels and user clearances.

A.2.2 Security Functional Requirements suitable to achieve the security objectives of the IT environment

This section provides the correlation and justification of suitability between the objectives for the IT environment and the Security Functional Requirements.

Security Objectives to be met by the IT Environment	Security Functional Requirement
OE.Key_Generation	Cryptographic key generation FCS_CKM.1

Table 6 - Correlation between Objectives of the IT environment and SFRs

OE.Key_Generation

FCS_CKM.1 ensures that cryptographic keys are generated with a specified algorithm and key size and conforms to given standards.

A.2.3 Security Assurance Requirements appropriate

The evaluation assurance level for this PP, namely EAL4 augmented (see [CC3] for a definition of EAL4), is the most appropriate because it is the minimum level that includes those elements of assurance mandated by the IPMAR standard. In particular the AVA_VLA.3 component was selected as more appropriate than AVA_VLA.2 (from EAL4) because the latter provides inadequate assurance of protection against physical attack, i.e. it only provides for resistance to attackers with a **low** attack potential.

A.2.4 Strength of Function claims appropriate

The claimed strength of function rating is SOF-medium. This is considered appropriate [CEM; Table B-2] for resistance to an attacker with attack potential of **moderate**.

A.2.5 Security Requirements mutually supportive

A.2.5.1 Requirements are mutually supportive and internally consistent

The following table gives the dependencies between the SFRs for the core model.

	ADV_SPM.1	AGD_ADM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1(1)	FDP_IFF.1	FDP_ITT.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1(1)	FMT_MSA.2	FMT_MSA.3(1)	FMT_SMR.2	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FAU_GEN.1																	x	
FCS_CKM.2			x	x						I			x	I	I			
FCS_CKM.3(1)			x	x						I			x	I	I			
FCS_CKM.3(2)			x	x						I			x	I	I			
FCS_CKM.4			x							I			x	I	I			
FCS_COP.1(1)			x	x						I			x	I	I			
FDP_ACC.1						x	I	I		I		I		I	I			
FDP_ACF.1					x		I	I		I		I		x	I			
FDP_DAU.1(1)																		
FDP_DAU.1(2)																		
FDP_IFC.1(1)								x										
FDP_IFF.1							x											
FDP_ITT.1					x					I		I		I	I			
FDP_ITT.3					x	I			x	I		I		I	I			
FDP_RIP.1(1)																		
FDP_RIP.1(2)																		
FIA_UAU.2										x								

	ADV_SPM.1	AGD_ADM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1(1)	FDP_IFF.1	FDP_ITT.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1(1)	FMT_MSA.2	FMT_MSA.3(1)	FMT_SMR.2	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FIA_UAU.6																		
FIA_UID.2																		
FMT_MOF.1										I					x			
FMT_MSA.1(1)					x	I				I				I	x			
FMT_MSA.2	x				x	I				I		x		I	x			
FMT_MSA.3(1)					I	I	I			I		x		I	x			
FMT_MTD.1(1)										I					x			
FMT_MTD.1(2)										I					x			
FMT_MTD.1(3)										I					x			
FMT_SMR.2										x								
FPT_AMT.1																		
FPT_FLS.1	x																	
FPT_PHP.1										I	x				I			
FPT_PHP.3(1)																		
FPT_PHP.3(2)																		
FPT_PHP.3(3)																		
FPT_RCV.1	x	x														I		x
FPT_RVM.1																		
FPT_SEP.1																		
FPT_STM.1																		
FPT_TST.1																x		
FTP_TRP.1																		

Table 7 - Dependency matrix for the core model

Key x - direct dependencies
I - indirect dependencies.

Note: For the Revenue-sensitive module interface information flow control policy (FDP_IFF.1) the only attributes are the inherent properties of the data and interfaces which may not be altered, therefore FMT_MSA.1 and FMT_MSA.3 have not been specified, and consequently indirect dependencies for this information flow control policy do not exist either.

All the dependencies (not explained by the above note) are satisfied by the TOE except the dependency on the key generation FCS_CKM.1 which is met by the TOE environment. FIA_UID.2 satisfies the dependencies on FIA_UID.1 as the former is hierarchic to the latter, and FMT_SMR.2 satisfies the dependencies on FIA_SMR.1 as the former is hierarchic to the latter.

The dependencies for the PP requirements augmented with the operating system functional package are given in the following table.

	ADV_SPM.1	AGD_ADM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1(1)	FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.2	FDP_ITT.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1(1)	FMT_MSA.1(2)	FMT_MSA.1(3)	FMT_MSA.2	FMT_MSA.3(1)	FMT_MSA.3(2)	FMT_SMR.2	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FAU_GEN.1																						x	
FCS_CKM.2			x	x								I		I			x	I		I			
FCS_CKM.3(1)			x	x								I		I			x	I		I			
FCS_CKM.3(2)			x	x								I		I			x	I		i			
FCS_CKM.4			x									I		I			x	I		I			
FCS_COP.1(1)			x	x								I		I			x	I		I			
FCS_COP.1(2)			x	x																			
FDP_ACC.1						x	I		I			I		I				I		I			
FDP_ACF.1					x		I		I			I		I				x		I			
FDP_DAU.1(1)																							
FDP_DAU.1(2)																							
FDP_DAU.1(3)																							
FDP_ETC.1								x		I		I			I	I			I	I			
FDP_IFC.1(1)									x														
FDP_IFC.1(2)										x		I			I	i			I	I			
FDP_IFF.1							x																
FDP_IFF.2								x				I			I	I			x	I			
FDP_ITC.1								x		I		I			I	I			x	I			
FDP_ITT.1					x							I		I				I		I			
FDP_ITT.3					x	I					x	I		I				I		I			
FDP_RIP.1(1)																							
FDP_RIP.1(2)																							
FIA_UAU.2												x											
FIA_UAU.6																							
FIA_UID.2																							
FMT_MOF.1												I								x			

	ADV_SPM.1	AGD_ADM.1	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1(1)	FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.2	FDP_ITT.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1(1)	FMT_MSA.1(2)	FMT_MSA.1(3)	FMT_MSA.2	FMT_MSA.3(1)	FMT_MSA.3(2)	FMT_SMR.2	FPT_AMT.1	FPT_STM.1	FPT_TST.1
FMT_MSA.1(1)					x	I						I						I		x			
FMT_MSA.1(2)								x				I								x			
FMT_MSA.1(3)								x				I								x			
FMT_MSA.2	x				x	I						I		x				I	I	x			
FMT_MSA.3(1)					I	I	I					I		x						x			
FMT_MSA.3(2)								I				I			x	x				x			
FMT_MTD.1(1)												I								x			
FMT_MTD.1(2)												I								x			
FMT_MTD.1(3)												I								x			
FMT_MTD.1(4)												I								x			
FMT_MTD.1(5)												I								x			
FMT_MTD.1(6)												I								x			
FMT_MTD.1(7)												I								x			
FMT_MTD.1(8)												I								x			
FMT_MTD.1(9)												I								x			
FMT_SMR.2												x											
FPT_AMT.1																							
FPT_FLS.1	x																						
FPT_PHP.1												I	x							I			
FPT_PHP.3(1)																							
FPT_PHP.3(2)																							
FPT_PHP.3(3)																							
FPT_RCV.1	x	x																			I		x
FPT_RVM.1																							
FPT_SEP.1																							
FPT_STM.1																							
FPT_TST.1																					x		
FTP_TRP.1																							

Table 8 - Dependency matrix for the augmented model

Key x - direct dependencies
I - indirect dependencies.

Note: The same comments apply for the Revenue-sensitive module interface information flow control policy.

All the dependencies (not explained by the above note) are satisfied by the TOE except the dependency on the key generation FCS_CKM.1 which is met by the TOE environment. FIA_UID.2 satisfies the dependencies on FIA_UID.1 as the former is hierarchic to the latter, FDP_IFF.2 satisfies the dependencies on FDP_IFF.1 (as required by FDP_IFC.1(2)), and FMT_SMR.2 satisfies the dependencies on FIA_SMR.1 as the former is hierarchic to the latter.

A.2.5.1 Justification that the SFRs form a mutually supporting and consistent whole

The security functional requirements split into a number of separate functional areas which leads to the absence of inconsistency and to a supportive relationship between themselves.

Thus, relevant security events are logged by the audit requirements which supports the other security functions.

The trusted path, and identification and authentication control access to the postage meter supports the access control policies and functions of users to the services of the meter. Access control and information flow policies, and their associated functions, further restrict the access to the revenue sensitive and cryptographic operation of the TOE to revenue officers. Similarly for the maintenance operations which are restricted to maintenance officers, but with the additional rules to zeroise critical data before allowing maintenance access - thus safeguarding the critical data from compromise whilst under maintenance control.

The integrity of postal indicia is guarded by monitoring the print transmissions and printing operations.

In the event that the additional functional package is used, MAC labelling provides an additional level of access control to critical data, and also protects the underlying software basis of the TOE by allowing authentication of the critical software images and restricting the operations on such images and to cryptographic information in primary and secondary memory to chosen operators.

The physical security of the TOE is maintained by policies and functions to safeguard the TOE against probing, tampering and environmental stress.

Enforcement requirements ensure the security functions of the TOE are not bypassed, whilst the Failsafe requirements ensure that the TOE remains secure in the event of error or at reset.

Cryptographic key generation takes place in the IT environment, whilst the other aspects of securing the key life-cycle such as distribution, entry and deletion are requirements of the meter. These support the cryptographic operations of the TOE which in themselves support many of the other security requirements such as data authentication.

These different functional areas, thus support each other, forming a cohesive, supportive and consistent whole.

B IPMAR TO PP CORRELATION

The following table provides a correlation between International Postage Meter Approval requirements of the Universal Postage Union [IPMAR] and the Security Functional and Assurance requirements of the PP.

Requirement	Satisfied by	Comment
1.01	ACM_CAP.4.6C	Assurance requirement refined.
1.02	ADV_HLD.3.9C ADV_LLD.1.10C	Specifically, refinement a) to both.
1.03	ADV_HLD.3.5C	
1.04	ADV_HLD.3.3C	Assurance requirement refined.
1.05	ADV_HLD.3.9C ADV_LLD.1.10C	Specifically, refinement b) to both.
1.06	ACM_CAP.4.6C ADV_SPM.1	Also the conformant ST will contribute to this.
1.07	ACM_CAP.4	
2.01	FPT_RVM.1	Satisfied by the refined SFR together with the assurance requirements that ensure it is upheld.
2.02	ADV_FSP.3.4C	Assurance requirement refined.
2.03	FDP_IFC.1 FDP_IFF.1	Part of the *Revenue-sensitive Module Interface information flow control* policy.
2.04	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
2.05	FMT_MOF.1	
2.06	FDP_RIP.1(1)	
2.07	AGD_ADM.1	
2.08	ADV_FSP.2.3C	
2.09	ADV_FSP.2.3C	Assurance requirement refined.
2.10	FDP_IFC.1 FDP_IFF.1	Part of the *Revenue-sensitive Module Interface information flow control* policy.
2.11	FTP_TRP.1.1	Functional requirement refined.

Requirement	Satisfied by	Comment
2.12	FDP_IFC.1 FDP_IFF.1	Part of the *Revenue-sensitive Module Interface information flow control* policy.
2.13	FDP_ITT.1 FDP_ITT.3	
2.14	ADV_FSP.3.4C	Follows automatically if a printing system is part of the TSF.
2.15	FDP_ITT.3	
2.16	FDP_ITT.1	
3.01	FMT_SMR.2	
3.02	AGD_ADM.1.4C	Assurance requirement refined.
3.03	FMT_SMR.2	
3.04	FMT_SMR.2	
3.05	FDP_RIP.1(1) FMT_SMR.2	
3.06	FDP_RIP.1(2)	
3.07	FPT_SEP.1	
3.08	ADV_HLD.3.3C ADV_HLD.3.8C	
3.09	FPT_AMT.1 FPT_TST.1	
3.10	ADV_DVS.1.1C	Assurance requirement refined.
3.11	FIA_UAU.6	
3.12	FMT_SMR.2.3	
3.13	FMT_SMR.2.3	
3.14	FIA_UAU.2 FMT_SMR.2.3	
3.15	FMT_SMR.2.3	
4.01	ADV_HLD.3.1C	Specifically, refinement a).
4.02	ADV_HLD.3.1C	Specifically, refinement b).
4.03	ADV_HLD.3.1C	Specifically, refinement c).

Requirement	Satisfied by	Comment
4.04	FPT_FLS.1 FPT_RCV.1 FPT_TST.1	
4.05	FIA_UAU.6	
4.06	ADV_HLD.3.1C	Specifically, refinement a).
4.07	ADV_HLD.3	Assurance requirement refined.
5.01	ADV_LLD.1	
5.02	FPT_PHP.3(1)	
5.03	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement a).
5.04	FPT_PHP.3(1)	
5.05	FPT_PHP.3(1)	
5.06	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
5.07	FPT_PHP.1	
5.08	FPT_PHP.3(1)	
5.09	FPT_PHP.3(1)	
5.10	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
5.11	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
5.12	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
5.13	FPT_PHP.3(2)	Specifically, FPT_PHP.3.1(2) refinement b).
5.14	FPT_PHP.1	
5.15	FPT_PHP.3(3)	
6.01	ADV_HLD.3 ADV_LLD.1	
6.02	ADV_RCR.2	
6.03	ADV_IMP.1	

Requirement	Satisfied by	Comment
6.04	ADV_IMP.1	Specifically, ADV_IMP.1.1C refinement a).
6.05	ADV_IMP.1	Specifically, ADV_IMP.1.1C refinement b).
7.01	FDP_DAU.1(3) FCS_COP.1(2) FMT_MTD.1(4) FMT_MTD.1(5) FMT_MTD.1(6) FMT_MTD.1(7) FMT_MTD.1(8) FMT_MTD.1(9) FPT_TRP.1	All but FPT_TRP.1 are included in the *Operating System functional package*.
7.02	FDP_DAU.1(2) FCS_COP.1(2) FPT_TST.1	All but FPT_TST.1 are included in the *Operating System functional package*.
7.03	FMT_MTD.1(4)	OS functional package.
7.04	FMT_MTD.1(5)	OS functional package.
7.05	FMT_MTD.1(6)	OS functional package.
7.06	FMT_MTD.1(7)	OS functional package.
7.07	FMT_MTD.1(8)	OS functional package.
7.08	FMT_MTD.1(9)	OS functional package.
7.09	FDP_IFF.1(2) FDP_IFF.2 FDP_ETC.1 FDP_ITC.1 FMT_MSA.3(2) FMT_MSA.1(2)	The B1 requirement has been stripped down to the minimum needed to satisfy the labelling requirements. It has been assumed there is no requirement to import or export labels with the information.
7.10	FTP_TRP.1	
7.11	FAU_GEN.1	
8.01	FDP_ACC.1 FDP_ACF.1	Part of the *Postal Meter Service* access control policy.
8.02	FDP_ACC.1 FDP_ACF.1	Part of the *Postal Meter Service* access control policy.

Requirement	Satisfied by	Comment
8.03	FDP_ACC.1 FDP_ACF.1	Part of the *Postal Meter Service* access control policy.
8.04	FDP_ACC.1 FDP_ACF.1	Part of the *Postal Meter Service* access control policy.
8.05	ADV_FSP.3 ADV_HLD.3 AGD_ADM.1	
8.06	FMT_MTD.1(1)	
8.07	FMT_MTD.1(2)	
8.08	FCS_CKM.1[E] FCS_COP.1 ADV_HLD.3 ADV_LLD.1	FCS_CKM.1 is a requirement on the IT environment which *may* be satisfied by a conformant TOE.
8.09	AVA_SOF.1 FMT_MSA.2	
8.10	FCS_CKM.3(1)	
8.11	FCS_CKM.3(1)	
8.12	FCS_CKM.2 ADV_HLD.3 ADV_LLD.1	
8.13	FCS_CKM.3(1)	
8.14	FCS_CKM.3(1)	
8.15	FDP_DAU.1(1) FCS_CKM.3(1)	
8.16	FCS_CKM.3(1)	
8.17	FDP_DAU.1(2)	
8.18	FCS_CKM.3(1)	
8.19	FIA_UAU.6	
8.20	FTP_TRP.1	
8.21	FDP_IFC.1(1) FDP_IFF.1	Part of the *Revenue-sensitive Module Interface information flow control* policy.
8.22	FDP_DAU.1(2)	

Requirement	Satisfied by	Comment
8.23	FCS_CKM.4 FMT_MTD.1(3)	
8.24	FCS_CKM.3(2)	
9.01	FCS_COP.1(1)	
10.01	N/A	EMI/EMC out of scope of the CC.
11.01	FPT_TST.1	
11.02	FPT_TST.1	
11.03	FAU_GEN.1 FPT_STM.1	
11.04	FAU_GEN.1	

Table 9 - Correlation between IPMAR and PP requirements