Stamps.com
Postage Server Cryptographic Module
Security Policy

(Non-Confidential)

Version 1.12

Table of Contents

1 Scope of Document

This document describes the Security Policy for the Stamps.com Postage Server Cryptographic module (PSC). The Security Policy specifies the security rules under which the PSC module operates. This document covers the security related services of the PSC module and is not intended to address non-security related PSC services or functions.

The PSC module is a cryptographic module, which implements the Data Encryption Standard, Secure Hash Standard, Data Authentication Code, and the Digital Signature Standard. It also implements ANSI X9.52 for Triple Data Encryption Algorithm Modes of Operation and FIPS PUB 112, Password Usage (See Section 2.1). The module provides services which can be used to support cryptographic based authentication, encryption applications, and postal meter secure operations.

2 Applicable Documents

- Performance Criteria for Information based Indicia-Open Systems, United States Postal Service
- Federal Information Processing Standards (FIPS) Publications (PUB) 140-1, Security Requirements For Cryptographic Modules, National Institute of Standards and Technology (NIST), 11 January 1994
- FIPS PUB 46-3, Requirements for 3DES, NIST, 1999
- FIPS PUB 112, Password Usage, National Bureau of Standards, 30 May 1985
- FIPS PUB 113, Computer Data Authentication, National Bureau of Standards, 30 May 1985
- FIPS PUB 180-1, Secure Hash Standard (SHA-1), NIST, 17 April 1995
- FIPS PUB 186, Digital Signature Standard, NIST, 19 May 1994

3 Cryptographic Boundary and Security Level

The PSC is a cryptographic module designed to meet the overall security requirements of FIPS 140-1 Security Level 3. The boundary of the cryptographic module is the coprocessor. Table 1 lists the security levels corresponding to each of the eleven security requirement sections of FIPS 140-1. The module does not contain an operating system; hence the requirements of that section do not apply.

Table 1: Module Security Level Specification

Security requirements section	Level
Cryptographic module	3
Module interfaces	3
Roles and services	3
Finite State Machine	3
Physical security	4
EFP/EFT	4
Software Security	3
Operating System Security	N/A
Key management	3
Cryptographic algorithms	3
EMI/EMC	3
Self-test	3

4 Roles and Services

The cryptographic module enforces access control using identity-based authentication, where each identified user has exactly one role. Service privileges are assigned to users based on their role. Every meter shall have a user chosen meter passphrase with a host-imposed level of entropy. User logon must always be based on their password.

- **Administrator (AD)**: Administrators manage the user profile database.
- **Auditor (AU)**: An Auditor manages (views, saves, archives, and deletes) audit logs.
- **Certificate Authority (CA)**: The Certificate Authority allows the meter's public key certificate to be loaded into the meter.
- **Customer (CU)**: The customer role is equivalent to the "User" role as defined in FIPS 140-1. The customer role always initiates from the host software.
- **Key Custodian (KC)**: Key custodians take possession of (encrypted) shares of keys during key export and enter them during key import.
- **Provider (PR)**: The provider role grants access to services that are required for performing meter provider functions; this is done inside the Stamps.com server infrastructure.
- **Security Officer (SO)**: The Security Officer role is equivalent to the Crypto Officer role as defined in FIPS 140-1. The Security Officer initiates key management functions, including import, export, activation and de-activation of keys.
- **No-Role (NR)**: These are services where authentication cannot be provided or is not required.

Table 2: Matrix of User Services and Roles

Services	Roles							
	Administrator	Auditor	Certificate Authority	Customer	Key Custodian	Provider	Security Officer	No-Role
Key Administration							X	
Authorize Customer						X		
Authorize PSD			X					
Administration Authorization							X	
Change User Password	X	X			X		X	
Session Management								X
Create User	X							
Create Audit Key							X	
Create Indicium				X				
Create Correction Indicium				X				
Withdraw PSD						X		
Delete User	X							
Request Device Audit								X
Download Postage Value						X		
Export Audit Key		X						
Key Exchange					X			
Logoff	X	X			X		X	
Logon								X

Services	Roles							
	Administrator	Auditor	Certificate Authority	Customer	Key Custodian	Provider	Security Officer	No-Role
Modify User	X							
Retrieve PSD Status				X				
Retrieve PSD Public Key								X
Set Clock	X							
Request Status	X	X	X	X	X	X	X	X
Update PSC							X	
View Users	X	X					X	

5 Security Rules

The security rules enforced by the Postal Service Cryptographic Module are enumerated below.

1. The cryptographic boundary shall consist of the coprocessor card including all software located inside the coprocessor.
2. Access control shall be identity based, where each identified user has exactly one role. Privileges are assigned to users based on their roles.
3. The cryptographic module supports a Customer Role (equivalent to the “user” role as defined in FIPS 140-1), the Security Officer Role (equivalent to the “Crypto-officer” role as defined in FIPS 140-1), the Provider Role, the Certificate Authority Role, the Key Custodian Role, the Administrator Role, and the Auditor Role.
4. The cryptographic module shall be limited to a single user at a time.
5. The cryptographic module shall allow the establishment of secure communication sessions between the coprocessor and the associated host computer.
6. The cryptographic module shall use the following FIPS 140-1 approved cryptographic algorithms: DES, DSA, RSA encryption (for key distribution), Triple-DES encryption, DES MAC, and SHA-1.
7. The cryptographic module shall perform self-tests on all cryptographic algorithms during power-up. The module shall perform KATs on DES, 3DES, RSA encryption, and SHA-1. The module shall also perform a pair-wise consistence test on the DSA algorithm.
8. The cryptographic module shall provide a “Show Status” service, which includes the current User ID and role, module state, session status, key management status (presence and status keys), and the time.

6 Security Relevant Data Items

Below is a brief description of the SRDIs protected by the PSC:

- **Audit key**: This key is used to sign audit records.
- **Registration keys**: These keys are used to protect data during registration.
- **Key encryption keys**: These keys are used to protect keys generated by the PSC.
- **User passwords**: These are user secrets used to perform identity-based authentication.
- **Provider authentication key**: This key is used to authenticate messages from the Provider.
- **CA authentication key**: This key is used to authenticate messages from the CA.
- **Customer authentication key**: This key is used to sign/authenticate messages to/from the Customer.
- **Customer encryption key**: This key is used to protect customer secrets.
- **Meter authentication keys**: These keys are used to sign/authenticate postal meter data.