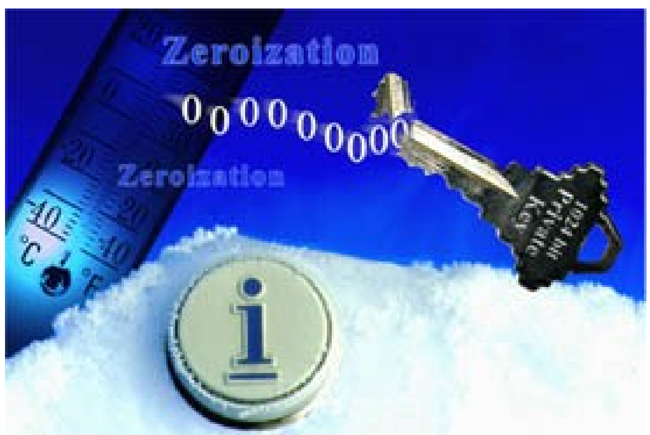
Pitney Bowes iButton Postal Security Device (PSD)

Hardware Version: MAXQ1959B-F50#
Firmware Version: 9.02.00
Indicia Type: 0, 1, 2, 5, 7 and 8



FIPS 140-2 Non-Proprietary Security Policy

Level 3 Validation
Document Version 1.2

June 11, 2014

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Pitney Bowes iButton Postal Security Device (PSD) hardware version MAXQ1959B-F50#, when loaded with firmware version – 9.02.00 and Indicia Type – 0, 1, 2, 5, 7 and 8. This security policy describes how the MAXQ1959B-F50# PSD iButton meets the security requirements of FIPS 140-2 as a multiple-chip standalone module. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module (plus Level 4 Environmental Failure Protection).

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/.

The MAXQ1959B-F50# PSD Postal Security Device is referred to throughout this document as the PSD, PSD iButton, and the module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Pitney Bowes website http://www.pb.com/cgi-bin/pb.dll/jsp/Home.do contains information on the full line of products from Pitney Bowes.

- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains a listing of validated modules that includes contact information for answers to technical or sales-related questions for the module.

MAXQ1959B#F50 PSD Postal Security Device iButton

Overview

An iButton® is a small hand held device that can be used to carry information. It is durable enough to be able to withstand everyday wear and tear much like the keys on a key chain. They can be dropped, stepped on, and even sent through the washer and dryer without compromising the information inside of the module.

A Postal Security Device (PSD) is an iButton that provides the same physical security of the standard iButton, and can also perform cryptographic functions. It also contains a tamper response system that will respond if the PSD is intentionally tampered with and zeroize all of the critical information contained on the module. This is provided as part of the module's mitigation of other attacks.

The MAXQ1959B-F50# PSD is designed to work within the Pitney Bowes Postage Meter System, where it can create and print indicia while keeping track of how much postage the iButton has used and how much it has remaining. The MAXQ1959B-F50# has been hardened to contain only the functionality necessary to perform the postal services, with only one PSD application locked on to the module.

The MAXQ1959#F50 PSD is manufactured for compliance to the Restriction of Hazardous Substances (ROHS) Act. A # sign is laser branded within the part number to indicate ROHS Compliance.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security Requirements	3 + EFP
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-tests	3
Design Assurance	3
Mitigation of Attacks	3

Table 1 - Cryptographic Module Security Levels

Module Interfaces

The cryptographic boundary of the MAXQ1959B-F50# PSD iButton is defined by the stainless steel metal MicroCAN®. There is one physical interface on the PSD iButton that is accessed through the steel lid contact. There are five different logical interfaces on the PSD iButton. The logical interfaces are: Data Input, Data Output, Control Input, Status Output, and Power.

The logical interfaces are kept logically separate by the 1-Wire® protocol which controls the physical and logical interfaces. The 1-Wire interface is implemented to control how information enters and exits the module. This interface only allows one communication (input/output) at any one given time, which separates the logically interfaces very efficiently.

The physical interface is separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Interface	FIPS 140-2 Logical Interface
Steel Lid Contact	Data Input Interface
Steel Lid Contact	Data Output Interface
Steel Lid Contact	Control Input Interface
Steel Lid Contact	Status Output Interface
Steel Lid Contact	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

Input and Output

All of the input and output to and from the module is done through the use of Application Protocol Data Units (APDU). The APDU is broken down into these sections:

- Class (CLA)
- Instruction (INS)
- Parameter 1 (P1)

- Parameter 2 (P2)
- Length of Data Command (Lc)
- Command Data (Data [Lc])

The first five define what type of command is being issued. The command data portion holds information that is needed to execute the command. Each service that is provided by the module requires a different APDU to execute the service.

Roles and Services

The module supports identity-based authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Provider (crypto-officer) Role and a User Role. All non-Approved services are explicitly indicated.

Provider (Crypto-Officer) Role

The Provider role can perform status checks, load postal configuration data, and generate key pairs. Service descriptions and inputs/outputs are listed in the table below.

The Provider functionality includes:

- Loading Postal Configuration Data
- Authorizing the module to the host
- Generating Keys
- Master Erase – Key Zeroization

A complete description of the Provider role services can be found in the Table 2. In this table, the input and output only depict the data part of the APDU. The first five sections defining which command is being issued is implied. In addition to the APDU, every operation also returns a status output indicating the status of the operation. If the operation completed successfully, the status output reflects this. If the operation is not completed successfully, the status output reflects this as well.

Role	Service	Description	Input	Output
Provider	Load Secret Key	Replace the current secret exchange key, provide a Keypad Refill Key, or keys specific to the non-US indicia formats	Secret Key Data Structure	None

Role	Service	Description	Input	Output
Provider	Generate Keys (non-(Approved)	Generates a DSA Key pair	Generate PSD Key Data	PSD Public Key Data Structure
Provider	Load Postal Configuration	Loads important module specific postal information to the module	Postal Configuration Data	None
Provider	Authorize	Authorizes the module to the host	PSD Certificate Data	None
Provider	Process PVD Message	Accepts a Postage Value Download Message from the host and increments the Descending register accordingly	Response Message	PB Data Center Status
Provider	Process PVR Message	Accepts the Postage Value Refund message from the host and adjusts the registers accordingly	Response Message	PB Data Center Status
Provider	Process Audit Response	Resets the Watchdog Timer by giving the PSD a valid response from the Provider	Audit Response Message	None
Provider	Verify Hash Signature	Verifies a hash signature	Verify Hash Signature Structure	None
Provider	Master Erase	Erases all information from the module, and transitions to the Transport PSD State.	Master Erase Data	None
Provider	Disable PSD	Places the PSD in a mode in which it cannot perform any Postal functions.	None	None
Provider	Enable PSD	Reverts the PSD to a mode in which it can carry out its Postal functions.	None	None

Table 3 - Provider Services, Descriptions, Inputs, and Outputs

User Role

The User role can perform status checks, basic postal functions, and self-tests. Service descriptions and inputs/outputs are listed in the table below.

The User functionality includes:

- Logging into/out of the module
- Creating Indicium
- Printing Indicium
- Adding/Removing Postage

A complete description of the User role services can be found in the following table. In this table, the input and output only depict the data part of the APDU. The first five sections defining which command is being issued is implied. In addition to the APDU, every operation also returns a status output indicating the status of the operation. If the operation completed successfully, the status output reflects this. If the operation is not completed successfully, the status output reflects this as well.

Role	Service	Description	Input	Output
User	Commit Transaction	Updates the Ascending and Descending registers and outputs the signed indicium	None	Signed Indicium Data
User	Create Indicium	Creates an Indicium using the input date	Postage Value, Date of Mailing, and Rate Category	Signed Indicium Data
User	Pre Compute R (non-Approved)	Pre computes the R portion of the DSA signature so that the create indicium function can be executed faster	None	A signed device audit message
User	Pre Create Indicium	Pre-creates the indicium based on the input values, and adjusts the pre-created register values	Postage Value, Date of Mailing, and Rate Category	None
User	Generate PVD Request	Makes a request to the host to download a Postage Value	Value of Postage Requested	Postage Value Download Request Message
User	Generate PVR Request	Generates a Postage Value Refund Request Message to send to the host	None	Postage Value Refund Request Message
User	Keypad Refill	Adds postage to the Descending register	Refill amount, and ASCII Combination Data	None
User	Keypad Withdrawal	Removes Postage from the Descending register	ASCII Combination Data	None
User	User Login	Authenticates the User to the module	Hash of Login Challenge and User Password	None
User	User Logout	Logs the user out, and returns the module to the Full Postal State	None	None

Table 4 – User Services, Descriptions, Inputs, and Outputs

Un-Authenticated Services

The PSD iButton provides several un-authenticated services. These services consist of basic status inquiries that do not require authentication and are available from any state of operation. The Run Self Tests service is also available from any state in the module, and does not require authentication. These services are detailed in the following table.

Role	Service	Description	Input	Output
All Roles	Get State	Returns the state that the Module is currently in.	None	The current state
All Roles	Create Device Audit Msg	Sends the value of the Ascending and Descending registers to the provider	None	Device Audit Message
All Roles	Run Self Tests	Runs the Self Tests	None	None
All Roles	Get Module Status	Returns the values of the Ascending and Descending registers	None	The values of the Ascending and Descending registers
All Roles	Get Challenge	Returns the most recent Login Challenge	None	The Value in the Login Challenge Variable
All Roles	Get PSD Parameters	Outputs the PSD Parameters List Structure	None	PSD Parameters List Structure
All Roles	Set GMT Offset	Sets the Local time offset from the GMT Time.	GMT offset in seconds	None
All Roles	Get Firmware Version	Returns the Firmware Version String	None	Firmware Version String
All Roles	Get Free RAM	Returns the number of free bytes of RAM	None	Number of bytes of free ram
All Roles	Get RTC	Returns the value of the Real Time Clock	None	The number of seconds since the battery was attached
All Roles	Get POR Count	Returns the number of Power On Resets since the battery was attached	None	Number of Power On Resets since the battery was attached
All Roles	Get Salt	Returns a non-cryptographic value used for salt and nonce values	A request for N bytes salt/nonce value	N byte salt/nonce value
All Roles	Get Log Data	Returns the contents of a specified log	Parameter to indicate which log to return	Contents of the appropriate log
All Roles	Get PSD Key Data	Returns the PSD Public Key if the PSD has been authorized	None	The PSD Public Key

Table 5 – Un-authenticated Services, Descriptions, Inputs, and Outputs

Authentication Mechanisms

Authenticating to the module is done through either challenge response or by asymmetric signature. The Provider (Crypto-Officer) and User authenticate through identity-based authentication, by demonstrating knowledge of the following keys and CSPs:

Provider Role: 1024-bit prime DSA key pair and/or a 128-bit 2-key Triple-DES key

User Role: 8-byte password and/or a 128-bit 2-key Triple-DES key

The types of authentication are listed in the table below.

Authentication Type	Strength	Roles
Provider Signature Verification	The module uses the Provider Public Key to verify the signature on input commands and authenticates the operator based on the signature verification. The 1024-bit DSA key provides 80-bits of equivalent symmetric strength providing a 1/(2^80) strength of authentication.	Provider Role
Triple-DES MAC Verification	The module uses the Provider Authentication Key to verify the 4-byte truncated MAC on input commands and authenticates the operator based on truncated MAC verification.	Provider Role
User Password Authentication	The User Password is 8 bytes long, and it is hashed with a random challenge that is 8 bytes long. These are both hashed with SHA-1 to create a 20-byte login command used to authenticate the user. Because the password is 64 bits, the strength of this authentication is a 1/(2^64).	User Role

Table 6 – Estimated Strength of Authentication Mechanisms

Physical Security

The MAXQ1959B-F50# PSD iButton is a multi-chip standalone cryptographic module. The cryptographic boundary for the module is the steel enclosure that makes up the iButton. The PSD iButton is contained inside a steel case that is strong, without any doors or hinges to open to access the module. It does not have any ventilation holes that allow an unauthorized user to gain access to the module. The iButton has a tamper response mechanism that zeroizes all information if an attempt to tamper the module has occurred. This is provided as part of the module's mitigation of other attacks.

The United States Postal Service requires that devices involved with the Information Based Indicia Program (IBIP) must meet the physical requirements for FIPS 140-2 Level 3. In addition to the level 3 requirements, all modules must be tested for EFP, which is a level 4 requirement for FIPS.

The MAXQ1959B-F50# conforms to the USPS standard by undergoing EFP Tests in addition to meeting the requirements for a FIPS 140-2 Level 3 Validation. The module is design to perform zeroization when operating outside the normal temperature operating range between -50°C and 125°C and in the voltage range of ±4 Volts. These tests have been conducted by the testing laboratory.

Cryptographic Key Management

FIPS Approved Algorithms

The module supports the following FIPS approved algorithms:

- SHS (Certificate #2286)[1]
- RNG (Certificate #1261)[2]
- Triple-DES (Certificate #1636)[3]
- DSA (Certificate #836)[4]
- HMAC (Certificate #1699)

[1] SHA-1 and SHA-256. SHA-1 approved for integrity and legacy digital signature verification.

[2] FIPS 186-2 RNG currently deprecated and will be disallowed after 2015

[3] Until December 31st 2015 two-key Triple-DES is allowed with the restriction that at most 2^{20} blocks of data can be encrypted with the same key. Key establishment methodology provides 112-bits of encryption strength.

[4] DSA 1024 approved for legacy digital signature verification

Non-Approved Algorithms

The module also uses the following non-approved algorithms while operating in FIPS mode:

- DSA – Digital Signature Generation & Key Generation (Certificate #836)
- Non-deterministic Hardware RNG
- Non-approved Firmware RNG
- Triple-DES MAC (Non-Compliant)

The module supports the following critical security parameters:

Key	Key Type	Generation	Storage	Use
PSD Secret Exchange Key[1]	Two-key Triple-DES (112-bit)	External by User or Provider	Plaintext in non-volatile memory	Decrypt secret keys entered into the PSD
Keypad Refill Key	Two-key Triple-DES (112-bit)	External by User or Provider	Plaintext in non-volatile memory	Compute CBC-MAC for keypad type refill
PSD Private Key[2]	DSA key set (160-bit)	Internal – Uses the FIPS 186-2 DSA key generation method	Plaintext in non-volatile memory	Digital Signature
PSD Public Key	DSA key set (1024-bit)	Internal – Uses the FIPS 186-2 DSA key generation method	Plaintext in non-volatile memory	Provided to external operators for verification of signature generated using PSD Private Key
Provider Public Key	DSA key set (1024-bit)	External by Provider	Plaintext in non-volatile memory	Verify Provider signed messages
Provider Authentication Key	Two-key Triple-DES (112-bit)	External by Provider	Plaintext in non-volatile memory	Authenticate the Provider role.
French K-Fab-MA Key	Two-key Triple-DES (112-bit)	External – computed from a shared secret key and the PSD serial number	Plaintext in non-volatile memory	For PSDs configured for the French market to encrypt French K-MA Key.
French K-MA Key	Two-key Triple-DES (112-bit)	External – loaded upon installation at the customer site	Plaintext in non-volatile memory	For PSDs configured for the French market to compute a CBC-MAC.
Belgian MAC Key	Two-Key Triple-DES (112-bit)	External – loaded upon installation at the customer site	Plaintext in non-volatile memory	For PSDs configured for the Belgium market to compute a CBC-MAC.
HMAC Secret Key	Hashed-based MAC Key (160/256-bit)	External – loaded upon installation at the customer site	Plaintext in non-volatile memory	This value is used to calculate HMAC values for the NetSet2, Flex IBI Lite, MailMark, indicia.
Triple-DES MAC Secret Key	Two-key Triple-DES (112-bit)	External – loaded upon installation at the customer site	Plaintext in non-volatile memory	Value used by some indicia to calculate TDES MAC in place of HMAC
User Password	Password (64-bit)	External – Created by User	Plaintext in non-volatile memory	Use by the User login process
FIPS 186-2 X-KEY	FIPS 186-2 RNG Seed Key (20-byte)	Generated internally using non-approved RNG	Plaintext in non-volatile memory	Used as the seed key value for the FIPS 186-2 x-Regular RNG
FIPS 186-2 K-Key	FIPS 186-2 RNG Seed Key (20-byte)	Generated internally using non-approved RNG	Plaintext in non-volatile memory	Used as the seed key value for the FIPS 186-2 k-Regular RNG

Table 7 – Critical Security Parameters

[1] Note: The two-key Triple DES is used to encrypt secret keys only and guaranteed to not be used more than a dozen times during the lifetime of the module. This is procedurally controlled by the Provider (Cryptographic Officer). The plaintext, ciphertext pairs are not accessible.

[2] The module generates cryptographic keys whose strengths are modified by available entropy of the RNG (80-bits).

Key Entry and Output

Keys that are created externally from the module are never transmitted to the module in plaintext. Keys are encrypted with the (Two-key [112-bit] Triple-DES) PSD Secret Exchange Key and sent through the physical interface and are then decrypted and stored in plaintext in Non-volatile RAM. After a key has been stored on the module, it is never output for any reason.

Key Generation

The only key generated within the module is the PSD DSA key set. The PSD DSA key set is generated during the Generate Keys function, which can be executed in the Provider Role. To ensure that the key pair functions properly, a pairwise consistency check is performed on any DSA key set that the module creates before the pair is used.

Key Access

The following Table shows the type of access that various services have to the CSPs. Services not listed in the Table do not have access to CSPs.

	Load Secret Key	Generate Key	Authorize	Load Postal Config. Data	Process PVD Message	Process PVR Message	Process Audit Message	Verify Hash Signature	Disable PSD	Enable PSD	Master Erase	Commit Transaction	Create Indicium	Pre-Compute R	Keypad Refill	User Login	Get PSD Key Data
PSD Secret Exchange Key	W/X										W						
Keypad Refill Key	W										W				X		
PSD Private Key	X	W									W	X	X	X			
PSD Public Key		R/W	X					X			W						R
Provider Public Key	X	X	X	X	X	X	X	X	X	X	W/X						
French K-Fab MA Key	W/X										W						
French K-MA Key	W										W						
Belgian MAC Key	W										W		X				
HMAC Secret Key	W										W		X				
TDES MAC Secret Key	W										W						
User Password											W					X	

Table 8 – Critical Security Parameter Access Table

Key Zeroization

Key zeroization can occur in two different ways. The first is through a master erase function call that can be called from any state after the module has been initialized. The master erase function removes all of the keys and critical security parameters from the module, and all of them must be entered again for the module to return to normal operation. The module must be returned to the manufacturer to be reinitialized.

The second method of zeroization is from a tamper event. If the module is tampered with, the tamper response system engages and zeroizes all of the information on the module. Once the module has been tampered, it cannot return to normal operation. This is provided as part of the module's mitigation of other attacks.

Self-Tests

The module performs the following Power-On Self Tests:

- CRC32 Firmware Image Tests – This test performs a cyclic redundancy check on the firmware image, and if it does not pass, the test fails.
- SHA-1 Known Answer Tests – This test performs a known answer test on the SHA-1 algorithm implemented by the module.
- HMAC SHA-1 Known Answer Tests – This test performs a known answer test on the HMAC SHA-1 implemented by the module.
- SHA-256 Known Answer Tests – This test performs a known answer test on the SHA-256 algorithm implemented by the module.
- HMAC SHA-256 Known Answer Tests – This test performs a known answer test on the HMAC SHA-256 implemented by the module.
- Triple-DES Known Answer Tests – This test performs a known answer test on the Triple-DES implemented by the module.
- RNG Known Answer Tests – This test performs a known answer test on all approved RNG algorithms implemented by the module.
- DSA Sign-Verify Tests – This test creates a DSA key pair, and tests the signing and verification processes with a known message.

If one of the Power-On Self Tests fails, then the module transitions to the Error state. From the error state, successfully passing the self-tests is the only way the module can transition back to the normal mode of operation.

The module performs the following Conditional Tests:

- Continuous RNG Tests for Firmware RNGs – This test is performed when a number is generated using any of the Firmware RNGs implemented by the module whether approved or non-approved.

- Continuous RNG Test for Hardware RNG - This test is performed when a number is generated using the Hardware RNG implemented by the module

- DSA Pairwise Consistency Tests

If the CRNGT for Firmware RNGs or DSA pairwise consistency test fail, an error is sent to the status output, and the module enters the same error state as the power-on self-tests.

If the CRNGT for the Hardware RNG fails, the module reports the error and attempts to generate a value again. If this generation fails three times, the module returns the error indicator and enters the same error state as the power-on self-tests.

Design Assurance

Maxim Integrated Products Inc. implements ISO-9000 for design assurance.

Mitigation of Other Attacks

The MAXQ1959B-F50# PSD iButton is designed to mitigate against side channel attacks.

The 1-Wire® interface transmits power and I/O; this complicates both monitor triggering and collection of data. Signal to noise on the single point of entry through the cryptographic boundary, obscures listening, and makes reception of critical data signals more difficult. The main processor is running while the coprocessor operates to introduce additional noise during strong source powered operation. This increased operating current may also improve the Signal/Noise ratio. The application storage of the FLASH-based PSD is locked during manufacturing precluding unauthorized operation or plain text attacks.

Additionally, the iButton provides extra physical protections against attacks beyond those required for Level 3 Physical Security. The iButton has a tamper response mechanism that zeroizes all information if an attempt to tamper the module has occurred.

FIPS 140-2 Operation of the PSD iButton

The MAXQ1959B-F50# PSD Postal Security Device has two roles, the Provider (Crypto-Officer) Role and the User Role. The PSD is powered on only once when the battery is attached during the manufacturing process.

The PSD iButton is a FIPS compliant device and it is considered to be operational when initialized during manufacturing with the Indicia Type of 0, 1, 2, 5, 7 or 8.

Provider (Crypto-Officer) Guidance

The provider should inspect the module upon receipt and ensure that there is no evidence of tampering. If there is evidence of potential tamper, then the module should be returned to Pitney Bowes.

Initialization

After the provider determines that the module is safe to use, they must initialize the module. This involves loading the postal configuration data and authorizing the module to the host. The postal configuration data includes the zip code, the maximum and minimum postage, and the vital information about the module that separates the module from others of the same type (e.g. serial number, etc.).

Zeroization

When the module has reached the end of its functional life cycle the provider shall perform a Master Erase on the module. The Master Erase zeroizes all information on the module so no unauthorized access can occur. After the Master Erase, the provider shall return the module back to Pitney Bowes.

If, for any reason, the module no longer functions properly, the provider shall return the module back to Pitney Bowes.

User Guidance

If, for any reason, the module no longer functions properly, the user shall return the module back to Pitney Bowes.

SECURE OPERATION

The MAXQ1959B-F50# PSD iButton meets Level 3 requirements for FIPS 140-2. The sections below describe how to verify that the module is operating in its FIPS-approved mode of operation.

FIPS Mode Indicator

The module supports a single mode of operation in which the module alternates service by service between Approved and non-Approved modes of operation. When the module executes the services not relying on cryptographic functions or relying on Approved algorithms it is said to operate in an Approved mode of operation. Corollary, when the services relying on non-Approved algorithms are executed, the module is said to operate in a non-Approved mode of operation. The module, **Firmware Version 9.02.00 and Indicia Type 0, 1, 2, 5, 7 and 8**, which is initialized during manufacturing is FIPS validated. If the module has been initialized during manufacturing to any other firmware version, such as the supported Indicia Type 6, it is not a FIPS validated module.

To determine if the module is in the FIPS mode of operation, the user of the module can call the GetFirmwareVersion function. In addition, calling the GetPSDParameters function (Field 16 of the return data structure PSD Parameter List Data) indicates the indicia type for which the module has been initialized. If the firmware version is 9.02.00 and the indicia type is 0, 1, 2, 5, 7 or 8, the module is validated.

ACRONYMS

ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DES/Triple-DES	Data Encryption Standard/Triple Data Encryption Standard
DSA	Digital Signature Algorithm
EFP	Environmental Failure Protection
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
IBIP	Information Based Indicia Program
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
POST	Power On Self Test
PSD	Postal Security Device
PVD	Postage Value Download
PVR	Postage Value Refund
RAM	Random Access Memory
RNG	Random Number Generator
ROHS	Restriction of Hazardous Substances
ROM	Read Only Memory
RSA	Rivest, Shamir, And Adleman
SHA	Secure Hash Algorithm