SafeNet DataSecure Appliance i150 and i450

FIPS 140-2 Level 2 Non-Proprietary Security Policy

DOCUMENT NUMBER:	002-010701-001
AUTHOR:	Iain Holness / Alan Frindell
DEPARTMENT:	Enterprise Engineering
LOCATION OF ISSUE:	Ottawa
DATE ORIGINATED:	July 30, 2009
REVISION LEVEL:	A
REVISION DATE:	March 24, 2011
SUPERSESSION DATA:	
SECURITY LEVEL:	

SafeNet, Inc. reserves the right to make changes in the product or its specifications mentioned in this publication without notice. Accordingly, the reader is cautioned to verify that information in this publication is current before placing orders. The information furnished by SafeNet, Inc. in this document is believed to be accurate and reliable. However, no responsibility is assumed by SafeNet, Inc. for its use, or for any infringements of patents or other rights of third parties resulting from its use. No part of this publication may be copied or reproduced in any form or by any means, or transferred to any third party without prior written consent of SafeNet, Inc.

TABLE OF CONTENTS

Section **Title** **Page**

1. INTRODUCTION 1
1.1 Purpose 1
1.2 References 1
1.3 Terminology 1
1.4 Document Organization 1
2. THE APPLIANCE 2
2.1 Cryptographic Module Specification 2
2.2 FIPS 140-2 Security Levels 3
2.3 Cryptographic Module Ports and Interfaces 3
2.3.1 i150 Interfaces 3
2.3.2 i450 Interfaces 4
2.4 Roles, Services and Authentication 5
2.5 Services for Authorized Roles 6
2.5.1 User 6
2.5.2 Administrator / Cryptographic Officer 7
2.5.3 Cluster Member 8
2.5.4 Recovery User 8
2.5.5 File Encryption User 9
2.6 Unauthenticated Services 9
2.7 Roles and Authenticated Services 9
2.8 Physical Environment 10
2.8.1 Tamper-Evident (TE) Labels 11
2.8.1.1. i150 TE Labels 11
2.8.1.2. i450 TE Labels 12
2.9 Operational Environment 13
2.10 Cryptographic Key Management 13
2.10.1 Key Generation 13
2.10.2 Key Access / Storage 13
2.10.3 Algorithms 14
2.10.4 Security Functions 14
2.10.5 Cryptographic Keys and CSPs 15
2.10.6 Access Control 16
2.11 Self-Tests 17

2.11.1 Power-On Self-Tests (POST) 17
2.11.2 Conditional Self-Tests 18
2.11.3 Mitigation of Other Attacks 18
3. FIPS APPROVED MODE OF OPERATION 19
3.1 Description 19
3.2 Invoking Approved Mode of Operation 19
3.3 Mode of Operation Indicator 19
3.4 Non-FIPS mode of Operation 19
4. GLOSSARY OF ACRONYMS, TERMS AND ABBREVIATIONS 20

LIST OF TABLES

Table Title Page
Table 2.2.1 – FIPS 140-2 Security Levels 3
Table 2.3.1 – FIPS 140-2 Logical Interfaces 5
Table 2.4.1 – Roles and Required Identification and Authentication 5
Table 2.4.2 – Strengths of Authentication Mechanisms 6
Table 2.5.1 – Authenticated User Services 7
Table 2.5.2 – Administrator / Cryptographic Officer Services 8
Table 2.5.3 – Cluster Member Services 8
Table 2.5.4 – Recovery User Services 9
Table 2.5.5 – File Encryption User Services 9
Table 2.6.1 – Unauthenticated Services 9
Table 2.7.1 – Roles and Authenticated Services 10
Table 2.8.1 – Inspection / Testing of Physical Security Mechanisms 11
Table 2.10.1 – FIPS Approved Algorithms 14
Table 2.10.2 – Non-FIPS Approved but Allowed Algorithms and Security Functions 14
Table 2.10.3 – Approved Security Functions 15
Table 2.10.4 – Non-Approved Algorithms used in non-FIPS Mode of Operation 15
Table 2.10.5 – Cryptographic Keys and CSPs 16
Table 2.10.6 – Public Keys Stored in Certificates 16
Table 2.10.7 – Access Control 17
Table 2.11.1 – Power-On Self-Tests 18
Table 2.11.2 – Conditional Self-Tests 18

LIST OF FIGURES

Figure 2.1.1 - Front View of the i150 2
Figure 2.1.2 – Front View of the i450 2
Figure 2.3.1 – i150 Front Controls (behind bezel) 3
Figure 2.3.2 – i150 Rear I/O Ports 3
Figure 2.3.3 – i450 Front I/O Controls and Display 4
Figure 2.3.4 – i450 Rear Panel 4
Figure 2.8.1 – i150 Chassis Side and Rear TE Labels 11
Figure 2.8.2 – i150 Chassis Right Side TE label 12
Figure 2.8.3 – i150 Chassis Left Side TE label 12
Figure 2.8.4 – i150 Rear TE Labels 12
Figure 2.8.5 – i450 Chassis Side and Rear TE Labels (rear view) 12
Figure 2.8.6 – Left Side of i450 12
Figure 2.8.7 – Right Side of i450 12
Figure 2.8.8 – TE label for Rear Tab of i450 12
Figure 2.8.9 –TE labels for i450 PSUs – 1st View 13
Figure 2.8.10 – TE Labels for i450 PSUs – 2nd View 13
Figure 2.8.11 – i450 Left Side Bezel Bracket TE Label 13
Figure 2.8.12 – i450 Right Side Bezel Bracket TE Label 13

1. INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the DataSecure Appliance i150 and i450. This security policy describes how the Appliance meets the security requirements of FIPS 140-2 and how to operate the Appliance in a secure FIPS 140-2 mode. This policy was prepared as a part of the Level 2 FIPS 140-2 validation of the Appliance.

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 NIST website at http://csrc.nist.gov/cryptval.

1.2 References

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

- The SafeNet Internet site contains information on the full line of security products at http://www.safenet-inc.com/products.
- For answers to technical or sales-related questions please refer to the contacts listed on the SafeNet Internet site at http://www.safenet-inc.com/company/contact.asp.

1.3 Terminology

In this document, when features common to both the DataSecure Appliance Models i150 and i450 are being discussed, then reference will be made to the “Appliance” or the “module”.

When the discussion is model-specific, then the Model i150 will be referred to as the “i150” and the Model i450 will be referred to as the “i450”.

1.4 Document Organization

The Security Policy document is part of the complete FIPS 140-2 submission package. In addition to this document, the complete submission package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Functional Specification
- Other supporting documentation as additional references

This document provides an overview of the Appliance and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the Appliance. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other validation submission documentation were produced by SafeNet. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 validation submission is proprietary to SafeNet and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact SafeNet.

2. THE APPLIANCE

2.1 Cryptographic Module Specification

The Appliance is a multi-chip standalone cryptographic module that is encased in a hard, opaque, commercial grade metal case, running a software solution that provides security and cryptographic processing. The cryptographic module also utilizes an internal server called the Network-Attached Encryption (NAE) Server, which executes a range of security-related tasks, including processing all cryptographic requests generated by NAE connectors residing on application servers and databases. The Appliance is a 1U device that fits into 1 space on a rack in a server room.

This document refers specifically to the Appliance versions i150 and i450 running firmware version 4.9.0.

DataSecure Appliance i150: HW P/N 947-00150-001; FW Version 4.9.0

DataSecure Appliance i450: HW P/N 947-000031-001; FW Version 4.9.0

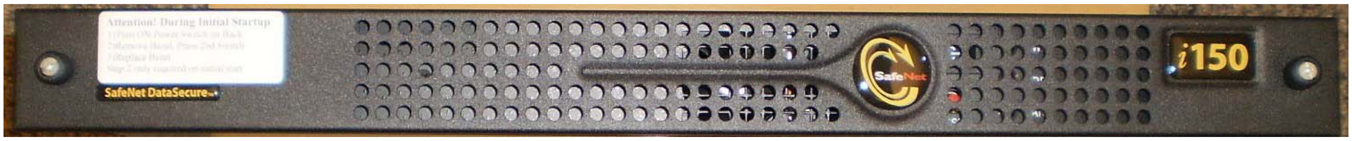


Figure 2.1.1 - Front View of the i150

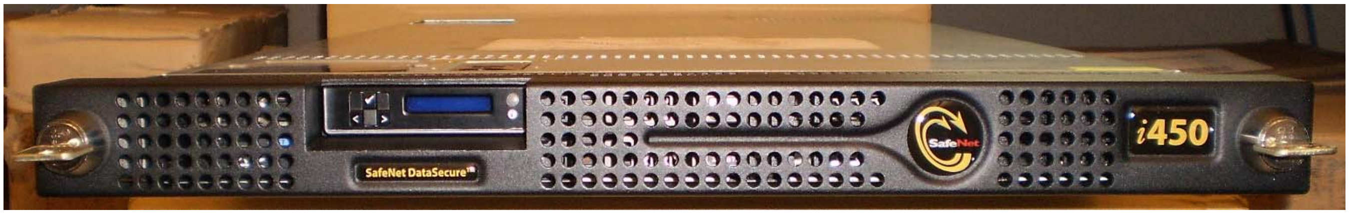


Figure 2.1.2 – Front View of the i450

The module provides key management (e.g. generation, storage, deletion, and backup), an extensive suite of cryptographic mechanisms, and process management including separation between operators.

The cryptographic module provides several interfaces for data input, data output, status output, and command input.

The Appliance is classified as a multi-chip standalone cryptographic module for FIPS 140-2 purposes. The FIPS 140-2 cryptographic boundary is defined by the perimeter of the metal case.

2.2 FIPS 140-2 Security Levels

The Appliance meets all level 2 requirements for FIPS 140-2 as summarized in Table 2.1:

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Machine	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI / EMC	2
9	Self Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Table 2.2.1 – FIPS 140-2 Security Levels

2.3 Cryptographic Module Ports and Interfaces

2.3.1 i150 Interfaces

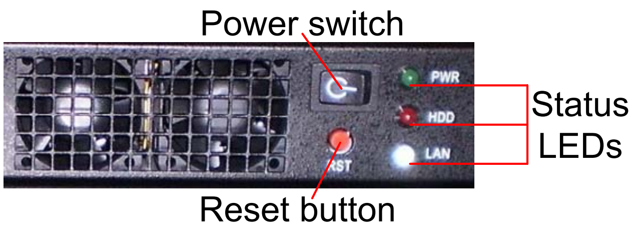


Figure 2.3.1 – i150 Front Controls (behind bezel)

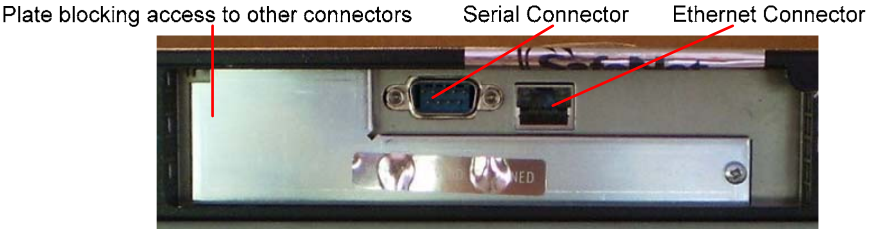


Figure 2.3.2 – i150 Rear I/O Ports

The i150 has the following ports and interfaces:

- Serial port (RS232 DB9)
- Network Interface Card (NIC) providing Ethernet at 10/100MBps
- VGA connector
- Power connector
- power button
- Reset (RST) button
- Power (PWR) status LED
- Hard drive activity (HDD) status LED
- Network activity (LAN) status LED (not operational)

2.3.2 i450 Interfaces

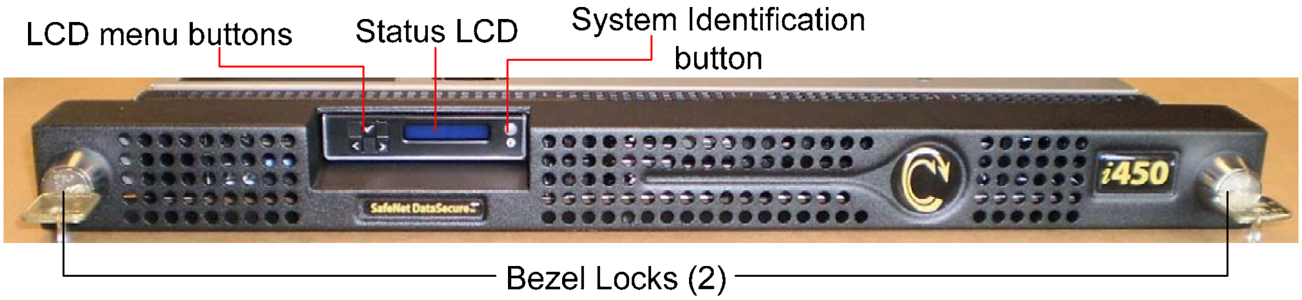


Figure 2.3.3 – i450 Front I/O Controls and Display

The front of the i450 has the following interfaces:

- Status LCD with 3 menu buttons
- System Identification button

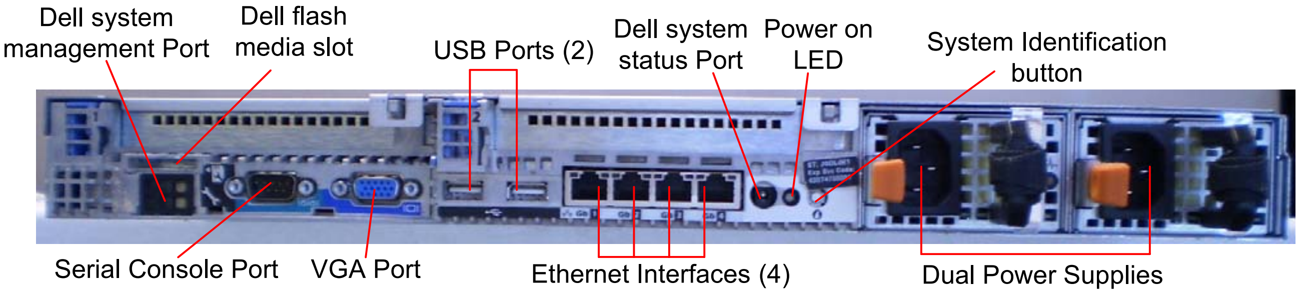


Figure 2.3.4 – i450 Rear Panel

The i450 has the following ports and interfaces:

- Serial port (RS232 DB9)
- 4 NICs providing Ethernet at 10/100/1000MBps
- VGA connector
- 2 Power connectors
- 2 Universal Serial Bus (USB) ports
- Power status LED
- Dell proprietary system management port, status port, flash media slot (not used but present)
- System identification button

All requests for services are sent to the Appliance via the NIC or serial port.

Note: The controls on the front of the Appliance are not used in lieu of remote management, hence the i150's front controls (Figure 2.3.1) are hidden behind a bezel while the i450 (Figure 2.1.2) only has the status LCD and system information buttons available.

The module's physical interfaces are separated into the logical interfaces, defined by FIPS 140-2, and described in Table 2.1:

FIPS 140-2 Logical Interface	Adapter Physical Interface
Data Input Interface	NIC, serial port
Data Output Interface	NIC, serial port
Control Input Interface	NIC, serial port, USB, LCD buttons
Status Output Interface	NIC, serial port, VGA, LCD display, status LEDs
Power Interface	Power connector

Table 2.3.1 – FIPS 140-2 Logical Interfaces

2.4 Roles, Services and Authentication

The Appliance supports identity-based authentication of multiple concurrent operator(s). Operators are identified by a username and password and/or certificate. The different roles and required authentication are shown in Table 2.4.1:

Role	Type of Authentication	Authentication Data
User	Identity-based	Username & password and / or public certificate
Administrator / Cryptographic Officer	Identity-based	Username & password and / or public certificate
Recovery User	Identity-based	Public certificate
Cluster Member	Identity-based	Public certificate
File Encryption User	Identity-based	Public certificate

Table 2.4.1 – Roles and Required Identification and Authentication

The module supports five distinct operator roles (User, Cryptographic Officer/Administrator, Recovery User, Cluster Member and File Encryption User). The cryptographic module enforces the separation of roles using identity-based operator authentication. An operator must enter a username and its password and/or provide a certificate to log in. The username is an alphanumeric string of one or more characters. The password is a string of eight or more characters chosen by the operator from the 90 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the logical interface that the operator is connected to. At the end of a session, the operator must log-out.

- Operators cannot change roles while logged in. They must log out first from the current role in use, then log in with the credentials of the role they wish to change to.
- Once the operator has been authenticated, the entered authentication data is cleared.
- Once the operator has logged out of their session, the keys that secured that specific session are cleared from the volatile memory. Likewise, if the module is powered-off at any given moment then the keys that secured all currently-active sessions (at that moment) are cleared as the volatile memory is cleared due to loss of power.

Authentication Mechanism	Strength of Mechanism
Password	Users, Administrators, and Cryptographic Officers (COs) accessing the module may be required to authenticate using a password that is at least 8-characters long. The characters used in the password must be from the 90 printable and human-readable ASCII characters. o This yields a minimum of 90^8 (or 4,304,672,100,000,000) possible combinations; thus the possibility of correctly guessing a password is less than 1 in 1,000,000. o After 5 failed authentication attempts, the account is locked out for 60 seconds; thus the possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. Note: the module suppresses feedback of authentication data being entered into the relevant interface by returning "*" characters.
Public Certificate	Recovery Users, Cluster Members and File Encryption Users must authenticate using a certificate (this is optional for Users, Administrators and COs). o 1024-bit or 2048-bit RSA certificates are used for SSL connections. o 1024-bit or 2048-bit DSA certificates are used for SSH connections. o The possibility of deriving a private RSA key is less than 1 in 1,000,000 and the possibility of randomly guessing the key in 60 seconds is less than 1 in 100,000. o The multi-step handshaking process for establishing a connection sets the possibility of randomly guessing the authentication data in 60 seconds at less than 1 in 100,000.

Table 2.4.2 – Strengths of Authentication Mechanisms

2.5 Services for Authorized Roles

2.5.1 User

This role is associated with external applications that connect via the module's XML interface.

This user is allocated all cryptographic services for keys that they have permission to access. The services available to an authenticated user are shown in Table 2.5.1.

Service	Description (if needed)
Encrypt Data	
Decrypt Data	
Sign Data	
Verify Data	
MAC Verify Data	
MAC Data	

Service	Description (if needed)
Export Encrypted Cryptographic Key	
Query Key Names	Outputs the list of key names and meta data that the user is allowed to access.
Export Certificate	Allows a User to export a certificate from the module.
Query Key Meta Data	Allows a User to output the following key information that he/she is allowed to access: key length, whether a key is exportable, whether a key can be deleted by current user, key permissions, and supported algorithms and modes for a key.
Generate Random Bytes	Allows a User to generate and return random data up to 2^{17} bytes in length.
Authenticate	Allows an operator to authenticate into the User role with a username and password. Authentication into the User role may also require an SSL tunnel to be created.

Table 2.5.1 – Authenticated User Services

None of the above services can be accessed until an operator successfully authenticates into a User role.

2.5.2 Administrator / Cryptographic Officer

This role is associated with Administrators / Cryptographic Officers (COs) who can access the module via the Web Management Console Interface (MCI) and/or the Command Line Interface (CLI).

This role provides all services that are necessary for the secure management of the module.

Service	Description
Key Management	Allows a CO to manage all cryptographic keys that are stored within the module. This includes the generation, storage, export (only public keys can be export directly), import, and zeroization of keys.
Update Firmware	Allows a CO to upgrade the module's firmware.
Cluster Management	Allows a CO to manage clusters. This includes the creation, joining, and removal of a cluster from the module.
Certificate Management	Allows a CO to create/import/revoke certificates within the module.
Service Management	Allows a CO to manage all services that the module supports. This includes the starting and stopping of all services.
Enable/Disable FIPS Mode	Allows the CO to configure the module into its FIPS validated configuration.
Operator Management	Allows a CO to create, modify, or delete module operators. The operators include Cryptographic Officers and Users.
Reset Factory Settings	Allows a CO to rollback to the default image that was shipped with the module.
Restore Default Configuration	Allows a CO to delete the current configuration file and restore the default configuration settings.

Service	Description
Restore Configuration File	Allows a CO to restore a previously backed up configuration file.
Backup Configuration File	Allows a CO to back up a configuration file.
Migrate DB	Allows a CO to encrypt and decrypt columns from a specific database.
Authenticate	Allows an operator to authenticate into the Administrator role with a username and password.
Zeroize Key(s)	Allows a CO to delete a specific key. When the CO chooses to zeroize all keys, the following happens: - the object master passwords for symmetric and asymmetric keys are zeroized - the key encryption keys for symmetric and asymmetric keys are zeroized - all rows in the relevant database tables are deleted

Table 2.5.2 – Administrator / Cryptographic Officer Services

2.5.3 Cluster Member

This role is associated with other Appliances that can connect to this module to create a cluster.

Service	Description
Receive Configuration File	Allows a Cluster Member to update the module’s configuration settings.
Zeroize Key(s)	Allows a Cluster Member to delete a specific key.
Backup Configuration File	Allows a Cluster Member to back up a configuration file.
Authenticate	Allows another module to authenticate into the module as a Cluster Member via an SSL tunnel. None of the above services can be accessed until another module is authenticated into the Cluster Member role.

Table 2.5.3 – Cluster Member Services

2.5.4 Recovery User

This role is associated with a Recovery user who can bring the module back into an “uninitialized state” in the event that all of the CO passwords are lost.

Service	Description
Authenticate	Allows an operator to authenticate into the Recovery User role with a signed token. None of the below services can be accessed until an operator has successfully authenticated as an Recovery User.
Restore Default Configuration	Allows an Recovery User to delete the current configuration file and restore the default configuration settings.
Reset Factory Settings	Allows an Recovery User to rollback to the default image that was shipped with the module.

Service	Description
Zeroize Key(s)	Automatically zeroizes all keys when Restore Default Configuration and Reset Factory Settings are activated.

Table 2.5.4 – Recovery User Services

2.5.5 File Encryption User

This role is associated with the File Encryption Connector running on a separate host on the same network as the module.

Service	Description
FE User Bootstrap	Accessed by a FE User as first time enrollment, using a shared secret to push a certificate to the FE User and allow use of the other services.
Authenticate	Allows the File Encryption Connector to authenticate into the module as a File Encryption User via a TLS tunnel. None of the below services can be accessed until the File Encryption Connector is authenticated into the File Encryption User role.
Request/Export Encrypted Key and Metadata	Allows a File Encryption User to request encrypted AES keys and metadata associated with the key.
Push Log Information	Allows a File Encryption User to push log files to the module regarding key usage by the File Encryption Connector.

Table 2.5.5 – File Encryption User Services

2.6 Unauthenticated Services

The cryptographic module supports the following unauthenticated services

Service	Description (if needed)
Health Status	Provides the current statistics of the cryptographic module.
Self-tests	Executes the suite of self-tests required by FIPS 140-2.
SNMP statistics	
Initiation of authentication mechanisms (e.g. TLS, SSH)	
Version negotiation of XML protocol	

Table 2.6.1 – Unauthenticated Services

2.7 Roles and Authenticated Services

Service	User	Administrator / CO	Cluster Member	Recovery User	FE User
Encrypt Data	●				
Decrypt Data	●				

Service	User	Administrator / CO	Cluster Member	Recovery User	FE User
Sign Data	●				
Verify Data	●				
MAC Verify Data	●				
MAC Data	●				
Export encrypted cryptographic Key	●				●
Query Key Names	●				
Export Certificate	●				
Query Key Meta Data	●				
Generate Random Bytes	●				
Authenticate	●	●	●	●	●
Key Management		●			
Update Firmware		●			
Cluster Management		●			
Certificate Management		●			
Service Management		●			
Enable/Disable FIPS Mode		●			
Operator Management		●			
Reset Factory Settings		●		●	
Restore Default Configuration		●		●	
Restore Configuration File		●			
Backup Configuration File		●	●		
Migrate DB		●			
Zeroize Key(s)		●	●	●	
Receive Configuration File			●		
FE User Bootstrap					●
Push Log Information					●
Request/Export Encryption Key and Metadata					●

Table 2.7.1 – Roles and Authenticated Services

2.8 Physical Environment

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

Production-grade components and production-grade opaque enclosure with tamper evident seals (for all module configurations) and locks on the front bezel (for the i450).

Physical Security Mechanism	Recommended Frequency of Inspection / Test	Inspection / Test Guidance Details
Tamper evident seals and locks on front bezel	6 months	Inspect the seals and/or locks on the front bezel, and the locks on the removable doors

Table 2.8.1 – Inspection / Testing of Physical Security Mechanisms

2.8.1 Tamper-Evident (TE) Labels

Each Model has its own unique configuration for Tamper Evident (TE) labels.

2.8.1.1. i150 TE Labels

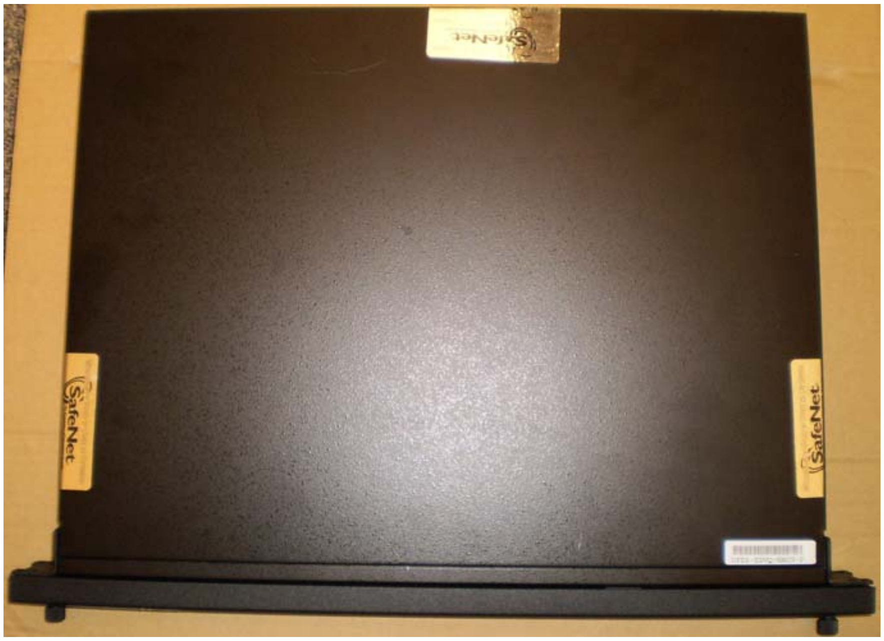


Figure 2.8.1 – i150 Chassis Side and Rear TE Labels

As indicated above and shown in the following figures, the i150 has TE labels in place to prevent:

- removal of the chassis lid
- removal of the plate blocking access to other connectors

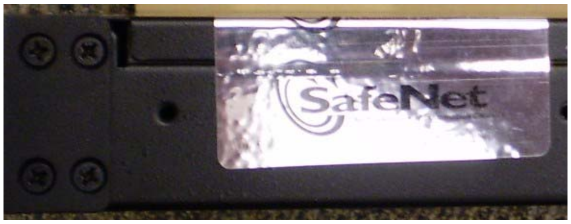


Figure 2.8.2 – i150 Chassis Right Side TE label

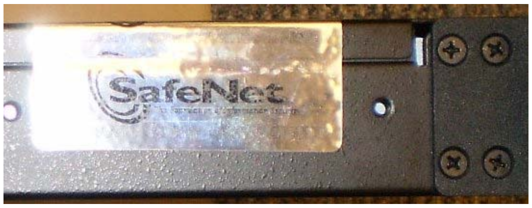
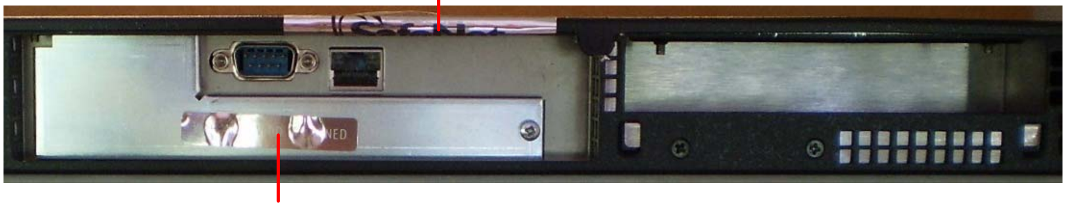


Figure 2.8.3 – i150 Chassis Left Side TE label

TE label preventing raising of chassis lid



TE label preventing removal of plate

Figure 2.8.4 – i150 Rear TE Labels

2.8.1.2. i450 TE Labels

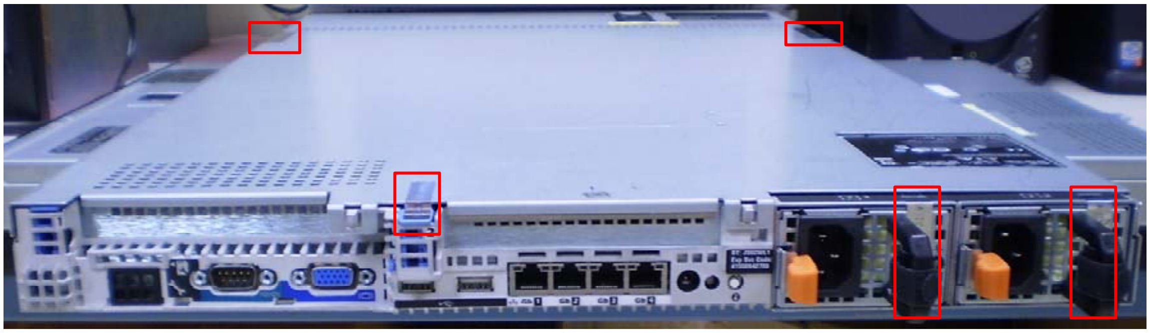
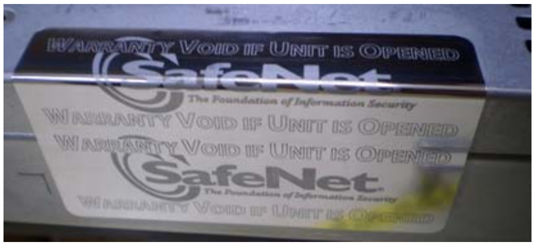
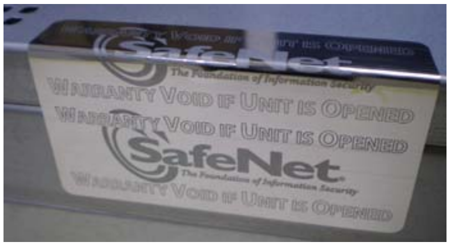


Figure 2.8.5 – i450 Chassis Side and Rear TE Labels (rear view)

As indicated in Figure 2.8.5 above and the following figures, the i450 has side and rear TE labels in place to prevent removal of the chassis lid and removal of each PSU (prevent access to the interior of the i450):


WARRANTY VOID IF UNIT IS OPENED
SafeNet
The Foundation of Information Security


WARRANTY VOID IF UNIT IS OPENED
SafeNet
The Foundation of Information Security

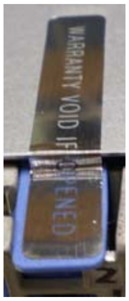


Figure 2.8.6 – Left Side of i450

Figure 2.8.7 – Right Side of i450

Figure 2.8.8 – TE label for Rear Tab of i450

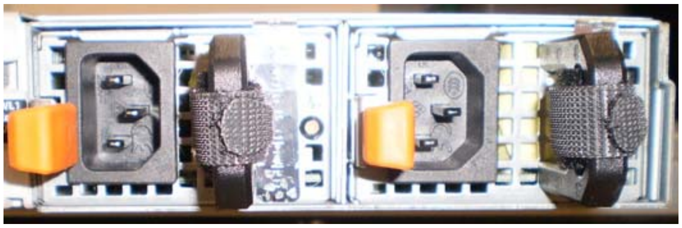


Figure 2.8.9 –TE labels for i450 PSUs – 1st View

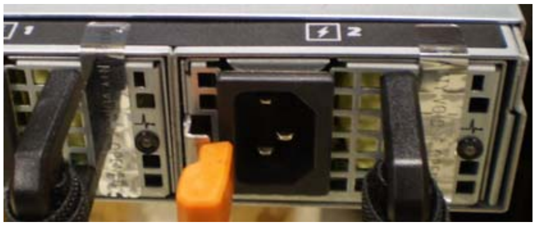


Figure 2.8.10 – TE Labels for i450 PSUs – 2nd View

Finally, to prevent removal of the front bezel, TE labels are applied as shown below.

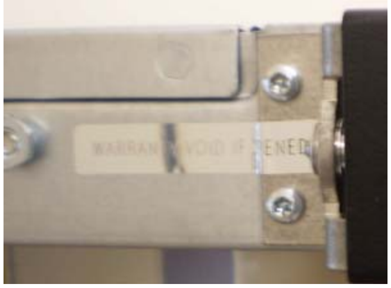


Figure 2.8.11 – i450 Left Side Bezel Bracket TE Label

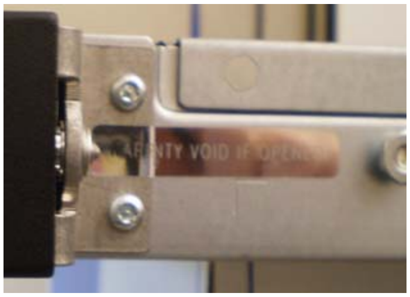


Figure 2.8.12 – i450 Right Side Bezel Bracket TE Label

2.9 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not contain a modifiable operational environment.

2.10 Cryptographic Key Management

The Appliance is a cryptographic management device that securely administers both cryptographic keys and other critical security parameters (CSPs) such as passwords.

2.10.1 Key Generation

The Appliance supports the generation of DSA, RSA and DH public and private keys. The module also supports the generation of Triple-DES keys as well as AES 128-bit, 192-bit and 256-bit keys. The module employs an ANSI X9.31 NDRNG for generating keys used in FIPS Approved algorithms.

2.10.2 Key Access / Storage

Keys are stored as encrypted data in database tables.

2.10.3 Algorithms

The module implements the following FIPS approved algorithms:

FIPS Approved Algorithm	Certificate
AES (FIPS PUB 197) ECB (e/d; 128,192,256) CBC (e/d; 128,192,256)	1315
Triple DES (FIPS PUB 46-3) TECB(e/d; KO 1,2); TCBC(e/d; KO 1,2)	916
Hashing SHA-1 (BYTE-only), SHA-256, SHA-384, SHA-512 HMAC SHA-1 (Key Sizes Ranges Tested: KS>BS) HMAC-SHA-256	1185 751 751
Random Number Generation ANSI X9.31 [TDES-2Key]	733
Digital Signatures Key Gen ANSI X9.31 (MOD: 1024,2048 | PubKey Values: 65537) Sig Gen PKCS#1/ Sig Ver PKCS#1 | 1024,2048 | SHA-1	421 629

Table 2.10.1 – FIPS Approved Algorithms

The module implements the following non-FIPS Approved but allowed algorithms:

Non-FIPS Approved but Allowed Algorithms and Security Functions
Key Agreement **Diffie-Helmann:** Diffie-Helmann within SSH (key agreement; key establishment methodology provides 80 bits of encryption strength) **RSA** key transport within TLS/SSL (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength) **NDRNG** for seeding the FIPS Approved RNG **MD5** within TLS/SSL

Table 2.10.2 – Non-FIPS Approved but Allowed Algorithms and Security Functions

2.10.4 Security Functions

The Appliance supports a wide variety of security functions. FIPS 140-2 requires that only FIPS Approved algorithms be used whenever there is an applicable FIPS standard.

Table 2.10.3 lists the Appliance approved algorithms. In the FIPS mode of operation only these Approved algorithms are available.

Approved Security Functions
Symmetric Key Encryption AES Triple-DES
Authentication RSA asymmetric key 1024/2048-bit (per ANSI X9.31) DSA asymmetric key 1024/2048-bits (per ANSI X9.31) SHA-1 SHA256, SHA384, SHA512 HMAC SHA-1 HMAC-SHA256
Key Generation Triple-DES/AES keys – PRNG (per ANSI X9.31) RSA keys – ANSI X9.31

Table 2.10.3 – Approved Security Functions

Table 2.10.4 lists the Appliance Non-Approved algorithsm used in the non-FIPS mode of operation.

Non-Approved Algorithms used in non-FIPS Mode of Operation
RSA 512, 768 DES SEED RC4 MD5

Table 2.10.4 – Non-Approved Algorithms used in non-FIPS Mode of Operation

2.10.5 Cryptographic Keys and CSPs

Data Item	Description
Database Key Encryption Key (KEK)	AES key used to encrypt and store symmetric keys and RSA private keys used via NAE Server in the database
Configuration KEK	Triple-DES key used to encrypt data stored in configuration files external to database
CA RSA Key	private signing key used by module to sign X.509 certificates and verify signatures on X.509 certificates signed by the CA running on the module
CA TLS Key	private part of the 1024/2048-bit RSA key pair used for TLS server authentication and key transport
CO Password	used to authenticate CO
User Password	used to authenticate User
Server SSH DSA Key	used to authenticate module for users establishing SSH connections

Data Item	Description
Server SSH RSA Key	used to authenticate module for users establishing SSH connections
SSH Session Key	used to encrypt SSH session data
TLS Session Key	Used to encrypt TLS session data
HMAC Key	Used to hash/verify input data
SSHv2 Diffie-Hellman Key	Diffie-Hellman key used to provide key establishment for SSHv2

Table 2.10.5 – Cryptographic Keys and CSPs

Data Item	Description
CA Verification Public Key Certificate (VPKC)	Public certificate used to verify CA's signature on signed X.509 certificates
TLS RSA VPKC	used for TLS server authentication and key transport as part of web administration and providing User cryptographic and cluster services
CO VPKC	optional: used if CO is required to authenticate to the module with a certificate
User VPKC	optional: used if User is required to authenticate to the module with a certificate
Cluster Member VPKC	used by Cluster Member to authenticate to the module
Recovery User VPKC	used by Recovery User to authenticate to the module
FE user VPKC	used by FE User to authenticate to the module
Firmware Update VPKC	used to verify signatures on uploaded firmware upgrades
SSHv2 Diffie-Hellman Public Key	used to provide key establishment for SSHv2
SSH RSA Public Key	used during SSH session
SSH DSA Public Key	used during SSH session

Table 2.10.6 – Public Keys Stored in Certificates

2.10.6 Access Control

Shows services from table x that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is **read** or referenced by the service.

W - The item is **written** or updated by the service.

X - The item is **executed** by the service. (The item is used as part of a cryptographic function.)

D - The item is **deleted** by the service.

Service	Authentication Data (Key or CSP)	Access Control
Authenticate User / Administrator / Crypto Officer	Password VPKC	R R

Service	Authentication Data (Key or CSP)	Access Control
Authenticate Cluster Member / Recovery User / FE User	VPKC	R
Encrypt Data	Database KEK	W,X
Decrypt Data	Database KEK	R,X
Sign Data	Database KEK	W,X
Verify Data	Database KEK	R,X
MAC Verify Data	Database KEK	R,X
MAC Data	Database KEK	W,X
Export encrypted cryptographic Key and Metadata	Database KEK	R
Export Certificate	VPKC	R
Query Key Meta Data	Database KEK	R
Key Management	Database KEK, Configuration KEK	R,W,D
Update Firmware	Firmware Upgrade KEK	R,X
Certificate Management	All VPKC	R,W,D
Operator Management	CO Password, CO VPKC User Password, User VPKC Cluster Member VPKC Recovery User VPKC File Encryption User VPKC	R,W,D R,W,D R,W,D R,W,D R,W,D
Reset Factory Settings	all	D
Restore Default Configuration	all	D
Restore Configuration File	Specific or all Configuration KEKs	R,W,D
Backup Configuration File	Specific or all Configuration KEKs	R,W
Migrate DB	all	R,W
Zeroize Key(s)	Specific or all keys	D
Receive Configuration File	Specific or all Configuration KEKs	R,W
FE User Bootstrap	File Encryption User VKPC, CA VPKC	R, W

Table 2.10.7 – Access Control

2.11 Self-Tests

Upon power-up the Appliance performs a number of power-up and conditional self-test to ensure proper operation.

2.11.1 Power-On Self-Tests (POST)

When the module is initially powered-on, it executes a battery of power-on self-tests. If any of these tests fail, the module will enter an error state and prohibit an operator from exercising the module's cryptographic functionality. No data is output by the module while these tests are running. Table 2.11.1 lists the power-on self-tests:

Test	Function	FIPS 140-2 Required
Symmetric Cipher AES KAT	Performs known answer tests for AES	Yes
Symmetric Cipher TDES KAT	Performs known answer tests for TDES	Yes
RNG KAT	Statistical Chi Square	No
MAC and HMAC KATs	Performs known answer tests for: SHA-1, HMAC-SHA-1, HMAC-SHA256 SHA-256, SHA-384, SHA-512	Yes
Asymmetric Cipher KATs	Performs known answer tests for RSA operations	Yes
Sign/Verify KATs	Performs known answer tests for RSA, DSA	Yes
Diffie-Hellman KAT	Performs known answer tests for DH	Yes
SSH Key Derivation Function KAT	Performs known answer tests for SSH	No
Firmware Integrity Test	Performs CRC-16 and RSA signature verification)	Yes

Table 2.11.1 – Power-On Self-Tests

2.11.2 Conditional Self-Tests

Test	Function	FIPS 140-2 Required
Continuous RNG	Performs the FIPS 140-2 required continuous RNG check each time the module's NDRNG and DRNG are used to produce random data	Yes (DSA, RSA)
Pairwise Consistency	Runs a pairwise consistency check each time the module generates a DSA, RSA or DH public/private key pair	Yes
Firmware Load	Checks that firmware is digitally signed before it can be loaded.	Yes

Table 2.11.2 – Conditional Self-Tests

2.11.3 Mitigation of Other Attacks

The FIPS 140-2 Area 11 Mitigation of Other Attacks requirements are not applicable because the Appliance is not designed to mitigate any specific attacks outside the scope of FIPS 140-2.

3. FIPS APPROVED MODE OF OPERATION

3.1 Description

The Appliance allows Administrators the choice of employing a wide range of security technologies. To comply with FIPS mode of operation the Appliance must be configured in a secure manner. This includes operating with the following FIPS Approved algorithms:

- DSA with 1024-bit keys for digital signature generation and verification
- RSA with 1024-bit / 2048-bit keys for digital signature generation and verification
- Triple-DES (three key) for encryption and decryption
- Triple-DES (two key) for encryption and decryption
- AES for encryption and decryption
- SHA-1 for hashing
- SHA-256, SHA-384, SHA-512 for hashing
- HMAC-SHA-1 for hashing
- HMAC-SHA-256 for hashing
- ANSI X9.31 RNG for generation of all keys

As well as the following non-FIPS Approved but allowed algorithm:

- Diffie-Hellman for key agreement within SSH V2 protocol (tested key establishment provides 80 bits of encryption strength)

3.2 Invoking Approved Mode of Operation

Authorized users can set the module in FIPS mode by setting the ‘Set FIPS compliant’ button under the high security configuration tab in the MCI.

3.3 Mode of Operation Indicator

The module is in FIPS mode when:

- the ‘Set FIPS Mode’ button is enabled
- the High Security page indicates FIPS mode
- the FIPS status interface returns a status of being in FIPS mode

3.4 Non-FIPS mode of Operation

In non-FIPS mode, the module also provides the following non-FIPS Approved algorithms:

- RSA with 512-bit, 768-bit keys
- DES for encryption and decryption
- SEED
- MD5
- RC4

4. GLOSSARY OF ACRONYMS, TERMS AND ABBREVIATIONS

Term	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CLI	Command Line Interface
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
Triple DES (EDE)	Data Encryption Standard (Encrypt Decrypt Encrypt)
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
FE	File Encryption
HTTP	Hyper Text Transport Protocol
IPSEC	Internet Protocol Security
(H)MAC	(Hashed) Message Authentication Code
MCI	Management Console Interface
NAE	Network Attached Encryption
NIC	Network Interface Card
PEM	Privacy Enhanced Mode
PKCS	Public Key Cryptography Standard
POST	Power On Self Test
RSA	Rivest Shamir Adelman
SCP	Secure Copy
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
WAN	Wide Area Network
XML (RPC)	Extensible Markup Language (Remote Procedure Call)