SNAPfone
Security Policy

Document Version 1.8

Snapshield, Ltd.

November 29, 2005

TABLE OF CONTENTS

1. Module Overview

SNAPfone (HW P/N Snapfone Versions E & F, FW Versions 7.10.1 v_7101 & 7.10.1 v_7101p2p) is a multi-chip standalone, compact encryption termination unit capable of encrypting incoming and outgoing voice and fax communications over analog telephone lines. SNAPfone is connected by one RJ-11 cable to the telephone line and by another RJ-11 connector to the phone. Status output is shown on the SNAPfone display. Control input is inserted using the DTMF signals from the phone and by SNAPfone buttons.

Figure 1 – SNAPfone Image

2. Security Level

SNAPfone meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The module only supports an Approved mode of operation; therefore, the module only operates in an Approved mode. The cryptographic module only supports FIPS Approved algorithms as follows:

- Diffie-Hellman with 1024-bit keys (key agreement; key establishment methodology provides 80 bits of encryption strength)
- 192-bit 3DES for encryption (Cert. #302)
- SHA-1 for hashing Authentication information. (Cert. # 289)

The SNAPfone relies on the implemented deterministic random number generator (DRNG) that is compliant with FIPS 186-2 with 192-bit XKEY and underlying G function constructed from SHA-1 for generation of all cryptographic keys (Cert. #53)**.** DRNG is seeded with NDRNG.

Secure Mode Status Indicator

The module supports both secure and plaintext transmissions. To check the status of the call, the operator shall confirm that there is a "User-User" or "Secure: XXXX" message on SNAPfone's display for secured calls; otherwise, the call is not encrypted.

4. Ports and Interfaces

SNAPfone provides the following physical ports and logical interfaces:

RJ-11 terminal line:	Data input, Data output.
RJ-11 phone line:	Data input, Data output, Control input.
Buttons (Qty. 5):	Control input.
LCD:	Status output.
Power port:	Power input.
Serial port:	Manufacturing environment only.

5. Identification and Authentication Policy

Assumption of roles

SNAPfone supports two distinct operator roles (User and Cryptographic-Officer). The Cryptographic-Officer must enter a password to log in. The password is a string of up to eight characters. The valid characters are 0-9,*, # (total 12). At the end of a session, the operator logs-out by hanging up. The User role is defined as being the SNAPtrunk or another SNAPfone, which authenticate by means of a six-character Group Number.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Role-based authentication	8-character Password
User	Role-based authentication	6-character Group Number

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Group Number	The probability that a random attempt will succeed or a false acceptance will occur is $1/12^6$ which is less than 1/1,000,000. It takes approximately six seconds to establish a session for authentication. As a result, the module is limited to ten authentication attempts per minute. The probability of successfully authenticating to the module within one minute is $10/12^6$ which is less than 1/100,000.
CO Password	The probability that a random attempt will succeed or a false acceptance will occur is $1/12^8$ which is less than 1/1,000,000. After ten failed authentication attempts, the module must be power cycled. It takes approximately three seconds to power cycle the device and each attempt takes approximately one second. As a result, the module is limited to 45 authentication attempts per minute. The probability of successfully authenticating to the module within one minute is $45/12^8$ which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User	• Make Secure Call • Receive Secure Call
Cryptographic-Officer	• Change Group Number • Change Password • Change User parameters • View User parameters

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Cryptographic Officer Password – Used to authenticate the CO role.
- Group Number – Used to authenticate the User role.
- 3DES Key – Used to secure sessions.
- DH Private Key – Used as the private component during the Diffie-Hellman key agreement protocol.
- DRNG Seed Key – Used to seed the DRNG.
- DRNG state – Used during the DRNG Continuous RNG Test.

Definition of Public Keys:

The following are the public keys contained in the module:

- DH SNAPfone Public Key – Used as the SNAPfone's public component during the Diffie-Hellman key agreement protocol.
- DH Device Public Key – Used as the public component received from the other party during the Diffie-Hellman key agreement protocol.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Generate: Generate the CSP
- Establish: Establish the CSP
- Use: Use the CSP
- Destroy: Actively zeroizes the CSP
- Modify: Update the CSP

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
	X	Make Secure Call	Generate Diffie-Hellman Private Key. Establish 3DES Key. Use Group Number. Destroy 3DES and DH Private Key.
	X	Receive Secure Call	Generate Diffie-Hellman Private Key. Establish 3DES Key. Use Group Number. Destroy 3DES and DH Private Key.
X		Change User Parameters.	Use CO Password.
X		Change Group Number.	Use CO Password. Modify Group Number.
X		Change Cryptographic Officer Password.	Use CO Password. Modify CO Password.
X		View User Parameters	Use CO Password

Unauthenticated Services:

SNAPfone supports the following unauthenticated services:

- Show status: This service provides the current status of the SNAPfone.
- Make/Receive Call: This service allows an operator to make/receive a normal phone call without cryptographic processing.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be invoked on demand by power cycling the device or by typing "#*8378" (#*TEST) on the connected equipment.
- Zeroize: This service actively destroys all plaintext critical security parameters. This is invoked by typing "#*73838" (#*RESET) on the connected equipment.

7. Operational Environment

Not applicable. SNAPfone operates in a non-modifiable environment.

8. Security Rules

SNAPfone's design corresponds to the SNAPfone's security rules. This section documents the security rules enforced by SNAPfone to implement the security requirements of this FIPS 140-2 Level 2 module.

1. SNAPfone shall provide two distinct operator roles; these are the User role and the Cryptographic-Officer role.
2. SNAPfone shall provide role-base authentication.
3. SNAPfone shall encrypt the call data using the 3DES algorithm.
4. The 3DES key shall be agreed using Diffie-Hellman algorithm.
5. SNAPfone shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:
      2. 3DES Known Answer Test
      3. SHA-1 Known Answer Test
      4. DRNG Known Answer Test
      5. Firmware integrity test: 16-bit CRC.

   B. Conditional Self-Tests:

      1. Continuous NDRNG test
      2. Continuous DRNG test
      3. Exclusive Bypass Test

   C. Critical Function Test:

      1. Exclusive Bypass Test

6. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test.
7. The software prevents data output during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The keys are related to entity by memory location.
10. Secure Call Indicators:

Upon each secure communication (incoming and outgoing), the *SNAPfone* indicates in the following manner that security has been achieved:

a. Visual indicator: "**User-User**" or "**Secure: XXXX**" message in the *SNAPfone* LCD.

b. Audible indicator: Double beep when the security has been established.

c. Audible indicator: Beep every 30 seconds.

9. Physical Security Policy

SNAPfone uses an enclosure that is opaque within the visible spectrum. Tamper evident labels are used to detect tamper attempts.

Figure 2 – SNAPfone Label Placement

10. Mitigation of Other Attacks Policy

Not applicable. The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Table 6 - Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A