Snapshield
Keeping Secrets Secret

SNAPcell
Security Policy

Document *Version 1.7*

Snapshield

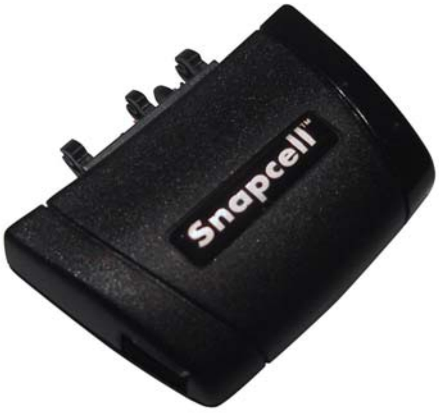
July 12, 2005

TABLE OF CONTENTS

1. Module Overview

SNAPcell (Firmware Version 5133 050322.2 SnapP2P.2 & 5133 050322.2 SnapP2MP.2, Hardware P/N Snapcell Version 1.5) is a multi-chip standalone encryption device for securing outgoing and incoming voice communications over a GSM connection by creating an encrypted communication channel with either the Encryption Center or another SNAPcell unit. The SNAPcell attaches to mobile phones through a mobile phone connector and the SNAPcell also provides a 2.5mm hands-free headset jack. The module provides status output via an LCD that is outside of the boundary and the single LED of the SNAPcell. The cryptographic boundary is defined as the outer perimeter of the plastic enclosure.

Figure 1 – SNAPcell Image



2. Security Level

SNAPcell 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 SNAPcell only supports an Approved mode of operation. As such, the module always operates in a FIPS Approved mode of operation. The cryptographic module supports the following FIPS Approved algorithms as follows:

- AES with 256-bit keys (Cert. #212)
- SHA-1 (Cert. #289).
- DRNG implemented in accordance to FIPS 186-2 with underlying G function constructed from SHA-1 (Cert. #53). The DRNG is seeded by a NDRNG.

The cryptographic module supports the following non-Approved algorithms:

- Diffie-Hellman with 1024-bit keys for key agreement

Instructions for Secure Operation

In order to place a Secure Call:

1. Click the headset button once.
2. Dial the destination number and select “Yes” on the mobile phone keypad.
3. Once the other party answers the call, a secure session will be initiated.

In order to receive a Secure Call:

1. Click the headset button once.

If a secure session is successfully established, the following indicators will confirm that the call is secured:

- Two beeps will be emitted through the headset initially
- An optional beep every 20 seconds may be configured
- The LED will be lit red,
- A message will be sent to the external phone LCD, “Secure Key: XXXX” for the SnapP2P.2 version or “User-User” for the SnapP2MP.2 version.

4. Ports and Interfaces

The SNAPcell supports a data input, data output, control input, status output, and power interface. The following physical ports and associated logical interfaces are supported:

- *Sony-Ericsson Mobile phone connector*: Data input, Data output, Control input, Status output, Power input
- *2.5mm Headset Jack*: Data input, Data output.
- *LED*: Status Output.

5. Identification and Authentication Policy

Assumption of roles

SNAPcell supports two distinct operator roles, the User and the Cryptographic-Officer. The Cryptographic-Officer is authenticated by entering an eight-digit password and is assumed by the human operator of the SNAPcell. The User is authenticated by providing a six-character Group Number and is assumed by a SNAPtrunk or another SNAPcell device.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Role-based authentication	Eight-digit Password
User	Role-based authentication	Six-character Group Number

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Group Number	The Group Number is a six-character secret chosen from a set of 94-alphanumeric characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/94^6, which is less than 1/1,000,000. Each User authentication attempt takes approximately six seconds. As a result, a maximum of 10 authentication attempts may be made in a minute. The probability of successfully authenticating to the module within one minute is 10/94^6, which is less than 1/100,000.
Password	The CO Password is an eight-digit number chosen from a set of 10-digits. The probability that a random attempt will succeed or a false acceptance will occur is 1/100,000,000 which is less than 1/1,000,000. After ten failed authentication attempts, the module must be power cycled before it accepts any further authentication requests. Power cycling the module takes approximately six seconds and each authentication attempt takes approximately one second. As a result, a maximum of 38 authentication attempts may be made in a minute. The probability of successfully authenticating to the module within one minute is 38/100,000,000, 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: Initiate an AES encrypted session. • Receive Secure Call: Receive an AES encrypted session.
Cryptographic-Officer	• Change Group Number: Update the Group Number, which is used for User authentication. • Change Password: Update the Password, which is used for CO authentication. • View/Change User Parameters: View and update non-security relevant configuration items. • Reset: Invoke on-demand power-on self-tests. • Zeroize: Actively zeroizes plaintext CSPs

Unauthenticated Services:

SNAPcell supports the following unauthenticated services:

- Show status: This service provides the current status of the cryptographic module through the mobile phone's LCD, the SNAPcell's LED, and the SNAPcell's 2.5mm headset jack.
- Power-up self test: Invokes on-demand power-on self-tests by power cycling the module.

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.
- AES 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 SNAPcell Public Key – Used as the SNAPcell'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 DH Private Key. Establish AES Key. Use Group Number. Destroy AES Key (at the end of the session). Destroy DH Private Key (at the end of the session).
	X	Receive Secure Call	Generate DH Private Key. Establish AES Key. Use Group Number. Destroy AES Key (at the end of the session). Destroy DH Private Key (at the end of the session).

X		View/Change User Parameters.	Use CO Password.
X		Reset	Use CO Password Destroy AES Key Destroy DH Private Key
X		Zeroize.	Use CO Password Destroy DRNG Seed Key Destroy DRNG State Destroy Group Number Destroy CO Password
X		Change Group Number.	Use CO Password Modify Group Number.
X		Change Password.	Use CO Password. Modify CO Password.

7. Operational Environment

The SNAPcell operates in a non-modifiable environment. As a result, the requirements of Area 6 of the FIPS 140-2 standard are not applicable.

8. Security Rules

This section documents the security rules enforced by the SNAPcell:

1. SNAPcell shall provide two distinct operator roles: the User role and the Cryptographic-Officer role.
2. SNAPcell shall provide role-base authentication.
3. SNAPcell shall secure data sessions using the AES algorithm.
4. The AES key shall be agreed using Diffie-Hellman algorithm.
5. SNAPcell shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      a. AES Known Answer Test.

      b. SHA-1 Known Answer Test.

      c. DRNG Known Answer Test.

2. Firmware integrity test: 16-bit EDC.

B. Conditional Self-Tests:

1. Continuous NDRNG test**.**
2. Continuous DRNG test**.**

6. The operator shall be capable of commanding the module to perform the power-up self-test by power-cycling the module. In addition, the CO may invoke the “Reset” command to invoke self-tests.
7. The module inhibits all 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 module does not support manual key entry.
10. The module does not support a maintenance role or interface.
11. The module does not support a bypass service.

9. Physical Security

The SNAPcell enclosure consists of two hard, opaque, plastic halves that encompass all components of the module. The two halves are ultrasonically welded together and cannot be separated without causing evidence of tamper.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
N/A	N/A	*N/A*

10. Mitigation of Other Attacks Policy

The SNAPcell is not designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

Table 7 – Mitigation of Other Attacks

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

11. Definitions and Acronyms

AES	Advanced Encryption Standard
CO	Cryptographic Officer
DH	Diffie-Hellman
DRNG	Deterministic Random Number Generator
LCD	Liquid Crystal Display
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
P2MP	Point-to-Multi-Point
P2P	Point-to-Point
SHA	Secure Hash Algorithm
USB	Universal Serial Bus