SkyTel ST900 Secure 2Way

Security Policy

Document *Version 0.3*

October 12, 2005

TABLE OF CONTENTS

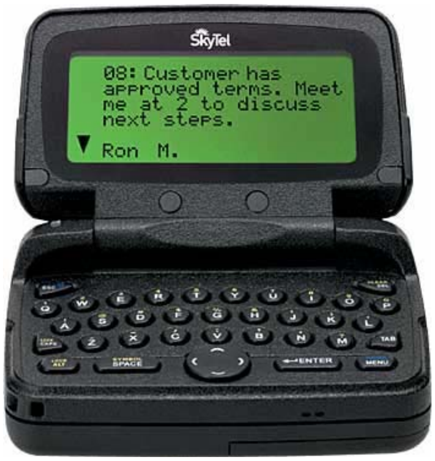
1. Module Overview

The SkyTel ST900 Secure 2Way (HW P/N ST900 Version 2.0; FW Versions 20050624 ver.f.2.9, 20050705 ver.f.3.0) is a multi-chip standalone cryptographic module encased in a hard, opaque, tamper-evident, commercial grade plastic case. The primary purpose for this device is to provide data security for narrow-band PCS [ReFLEX] traffic. The device provides a data input, data output, control input, status output, and power interface via its physical ports. The cryptographic boundary is defined as the outer perimeter of the plastic enclosure, but excludes the following components from the cryptographic boundary:

- External Battery: Non-security relevant. Does not provide any cryptographic services or perform cryptographic processing. Does not have any association or access with CSPs.
- LCD: Non-security relevant. Does not provide any cryptographic services or perform cryptographic processing. Does not have any association or access with CSPs.
- RF Module: Non-security relevant. Does not provide any cryptographic services or perform cryptographic processing. Does not have any association or access with CSPs and is an off-the-shelf product.

The image below illustrates the cryptographic boundary:

Figure 1 – Image of the SkyTel ST900 Secure 2Way



SkyTel
08: Customer has approved terms. Meet me at 2 to discuss next steps.
Ron M.

2. Security Level

The cryptographic module 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	2
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	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

The cryptographic module only supports a FIPS mode of operation. The following FIPS Approved algorithms are supported:

- AES (128-bit, ECB, CTR mode) for encryption/decryption
- HMAC SHA-1 for data integrity
- SHA-1

The cryptographic module also implements a deterministic random number generator (DRNG) that is compliant with ANSI X9.31. In addition to the FIPS Approved algorithms, the SkyTel ST900 Secure 2Way also supports the following non-Approved key agreement protocol that meets the requirements of FIPS 140-2 Annex D:

- EC-DH (key agreement methodology provides 80 bits of encryption strength)

4. Ports and Interfaces

The SkyTel ST900 Secure 2Way provides the following physical ports and logical interfaces:

LCD Connector:	Data output, Status output
Serial port (RS232):	Power input, Data input, Control input, Data output, Status output
RF Module Connector:	Data input, Data output, Control input, Status output
Battery Connector:	Power input
Keypad:	Data input, Control input
LED:	Status output
Buzzer:	Status output

5. Identification and Authentication Policy

Assumption of roles

The SkyTel ST900 Secure 2Way shall support two distinct operator roles (User and Cryptographic-Officer). The cryptographic module shall enforce the separation of roles using role-based operator authentication. The Cryptographic-Officer authenticates to the module by proving knowledge of an 80-bit shared HMAC SHA-1 secret or a 24-bit password on a per-command basis; while the User authenticates to the module via an 8-character password (Maximum password length is 12-characters). The password is an alphanumeric string of characters randomly chosen from 78 printable and human-readable characters. Upon correct authentication, the role is selected based on the authentication data of the operator. The cryptographic module does not retain previous authentications across power cycles.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication	Password
Cryptographic-Officer	Role-based operator authentication	Knowledge of a shared HMAC SHA-1 secret or password

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/78^{8}, which is less than 1/1,000,000. After 20 successive failed authentication attempts, the SkyTel ST900 Secure 2Way will render itself inoperable. The probability of successfully authenticating to the module within one minute is 20/78^{8}, which is less than 1/100,000.
Knowledge of 80-bit Shared HMAC SHA-1 Secret or 24-bit Password	The probability that a random attempt will succeed or a false acceptance will occur is at least 1/2^{24}, which is less than 1/1,000,000. Due to network latency, the SkyTel ST900 Secure 2Way will only permit three attempts per minute. The probability of successfully authenticating to the module within one minute is at least 3/2^{24}, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role is assumed by the end-user of the device.	• Update Password: Updates the User password with the newly specified password. • Login: Authenticate to the module upon power-up. • Secure Messaging: Services that allow the User to securely communicate with other devices using AES encrypted messages and also allows for User management of messages. • Messaging: This service allows an operator to perform

	unsecured messaging services and message management. • <u>User Preferences</u>: The User may configure certain non-security relevant settings to personalize the module.
Cryptographic-Officer: This role is assumed by the SkyTel Crypto Server.	• <u>Security Enable</u>: Configures the module to exclusively provide cryptographic services for message encryption/decryption and also performs key agreement. The module will indicate that message encryption has been enabled by displaying an icon of a lock on the external LCD. In addition, each encrypted message is displayed prefixed with an "S". • <u>Security Disable</u>: Configures the module to exclusively provide clear-text messaging in a bypass mode of operation. • <u>Clear Memory</u>: The same as the Security Disable service, except that messages will also be erased from FLASH memory. • <u>Zeroize</u>: Actively overwrites all CSPs with 0's. • <u>Change Key</u>: Performs a new key agreement to replace the current key.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show status: This service provides the current status of the cryptographic module through the LCD, LED, and Buzzer.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling the module.
- Remote Device Administration: This service is provided to SkyTel for Over-The-Air-Programming of network subscriptions and general non-security relevant configuration settings.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- HMAC Shared Secret Key: This key is used with HMAC SHA-1 for data integrity and is also used to authenticate the Cryptographic Officer.
- CO Password: This CSP is used to authenticate the CO role.
- User Password: This CSP is used to authenticate the User role.
- AES Key: This key is used to encrypt/decrypt data traffic when the module is configured for data encryption.
- Internal State of the RNG: This CSP is used to seed the RNG during the next iteration.
- ECDH Private Key: Used during EC-DH key agreement.

Definition of Public Keys:

The following are the public keys contained in the module:

- ECDH Public Key: Used as the module's public portion during EC-DH key agreement.
- ECDH Server Public Key: Used as the CO's public portion during EC-DH key agreement.

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 – The CSP is generated or agreed upon during this service.
- Use – The CSP is accessed/used during this service.
- Modify – The CSP is modified during this service.
- Destroy – The CSP is destroyed/zeroized during this service.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
	X	Update Password	Modify User Password
	X	Login	Use User Password
	X	Secure Messaging	Use AES Key

	X	Messaging	None
	X	User Preferences	None
X		Security Enable	Generate AES Key, Use HMAC Shared Secret Key, Use CO Password, Generate/Use ECDH Private Key, Use Internal RNG State
X		Security Disable	Use CO Password, Destroy AES Keys
X		Clear Memory	Use CO Password, Destroy AES Keys
X		Zeroize	Use CO Password, Destroy All CSPs
X		Change Key	Generate AES Key, Use HMAC Shared Secret Key, Generate/Use ECDH Private Key, Use Internal RNG State
		Show Status	None
		Self-Tests	None
		Remote Device Administration	None

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the SkyTel ST900 Secure 2Way does not contain a modifiable operational environment.

8. Security Rules

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

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic module shall provide role-based authentication.
3. The cryptographic module shall enforce User passwords to be a minimum of eight characters in length.
4. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall encrypt message traffic using the AES algorithm.
6. The cryptographic module shall perform the following tests:

A. <u>Power up Self-Tests:</u>

1. Cryptographic algorithm tests:

   a. AES Known Answer Test
   b. ANSI X9.31 DRNG Known Answer Test
   c. HMAC SHA-1 Known Answer Test
   d. SHA-1 Known Answer Test (Tested along with HMAC)

2. Firmware Integrity Test (16-bit EDC)
3. Critical Functions Tests
   a. EC-DH KAT
   b. Exclusive Bypass Test

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test

2. Exclusive Bypass Test

7. Data output shall be inhibited during, 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 shall support concurrent operators.
10. The module shall not support a maintenance role.
11. The module shall support an exclusive bypass capability.

9. Physical Security Policy

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.

Operator Required Actions

The operator is required to periodically inspect tamper evident seals.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
Tamper Evident Seal	1 month	*The tamper seal is located on the backside of the module, beneath the battery pack, and covering the three removable screws.*

10. Mitigation of Other Attacks Policy

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

11. Definitions and Acronyms

AES – Advanced Encryption Standard

BOM – Bill of Materials

CM – Configuration Management

CO – Cryptographic Officer

CSP – Critical Security Parameter

DRNG – Deterministic Random Number Generator

EC-DH – Elliptic Curve Diffie-Hellman

EDC – Error Detection Code

FSM – Finite State Model

IC – Integrated Circuit

LCD – Liquid Crystal Display

LED – Light Emitting Code

LCD – Liquid Crystal Display

RF – Radio Frequency

SHA – Secure Hash Algorithm