ND SatCom Products GmbH

SKYWAN Cryptographic Module

FIPS 140-2 Cryptographic Module Security Policy

TP2269E_0000103

Version: 1.4

Date: October 27, 2014

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the ND SatCom Products GmbH SKYWAN Cryptographic Module, hereafter denoted *the Module*. The Module is an embedded traffic processing engine for the SKYWAN satellite modem. The Module meets FIPS 140-2 overall Level 3 requirements.

Table 1 – Cryptographic Module Configurations

HW P/N and Version	FW Version
F-11B13860 (Vendor SAP Identifier) TQM8349L-CA rev. 300	Boot Loader FW version 2.002.4 Application FW version 7.250.10

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated satellite communications. The Module is a multi-chip embedded embodiment.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

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

1.1 Hardware and Physical Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The physical cryptographic boundary is the surface and edges of the epoxy covered PCB assembly. The Module relies on the SIC DEMOD carrier board as an input/output device.

The following are excluded from the cryptographic boundary:

4x switching regulator filters

1x capacitor

1x PCB trace for PCI sync in

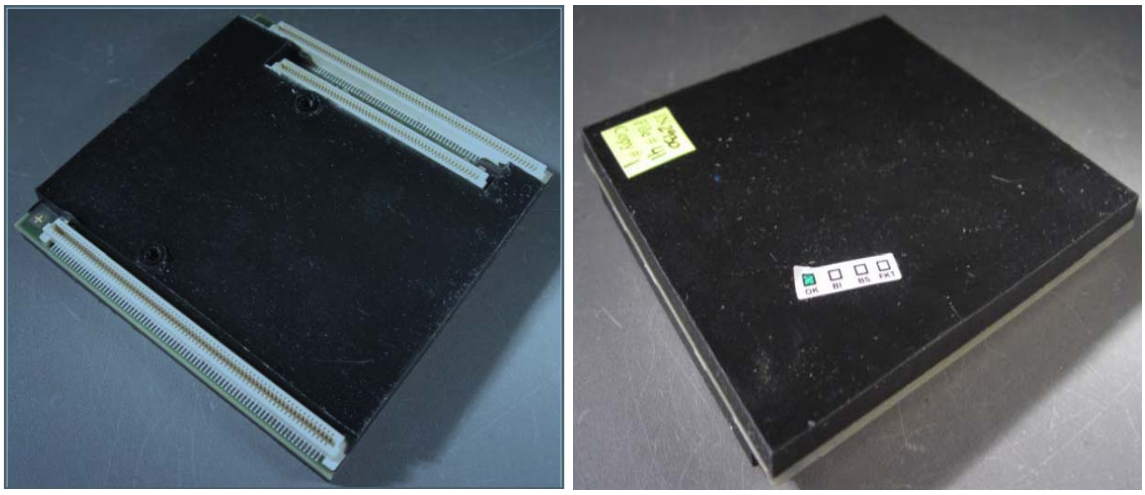

Figure 1 - Module top (left) and bottom (right)

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
PCI Bus	The PCI controller connects the processor and memory system to the I/O components through the PCI system bus. This bus is used as I/O between crypto module and SIC/DEMOD board.	Data in | Data out | Control in | Status out
Local Bus	Supports three interfaces: GPCM, UPM, and an SDRAM controller. This bus is used as I/O between crypto module and FPGA for TX/RX over the satellite.	Data in | Data out | Control in | Status out
General Purpose I/O / Timers	Each GPIO module supports 32 general-purpose I/O ports. Each port can be configured as an input or as an output.	N/A - Disabled by software.
USB	Implements two USB modules, a multi-port host (MPH) module and a dual-role (DR) module	N/A - Disabled by software.
Interrupt controller	Provides interrupt management that is responsible for receiving hardware-generated interrupts.	N/A - Disabled by software.

Port	Description	Logical Interface Type
Ethernet / TSECs	This three-speed Ethernet controller (TSEC) implements a gigabit Ethernet protocol.	N/A - Disabled by software.
I2C	The inter-IC (IIC or I2C) bus is a two-wire—serial data (SDA) and serial clock (SCL)—bidirectional serial bus that provides a data exchange between this device and other devices.	N/A - Disabled by software.
SPI	The SPI is a full-duplex, synchronous, character-oriented channel that supports a four-wire interface (receive, transmit, clock and slave select).	N/A - Disabled by software.
Clock, Reset & Power Management	The reset, clocking, and control signals offer many options for the operating the device.	Control in | Status out
DUART	The DUART consists of two (dual) universal asynchronous receiver/transmitters (UARTs). Used RS485 M&C protocol (no security relevant data)	Control in | Status out
Power Supply	Supplies 3.3V, 2.5V, 1.25V, and 1.2V	Power in
JTAG	This port/interface is Hardware Disabled	N/A – Hardware disabled.

1.2 Mode of Operation

The Module operates only in the FIPS 140-2 Approved mode of operation. The period of initialization for the Module (IG 9.5) includes the firmware load operation, in which the entire Application image is copied from a memory external to the Module. To verify that the Module is in the Approved mode of operation, the unauthenticated Show Status service can be invoked. The high-level log files will have an entry clearly stating that the Module is in the FIPS-140-2 Approved mode of operation. Additionally, the SNMPv2 read only OIDs can be used to verify that the module is in the Approved mode of operation.

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 4 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB Key sizes: 256 bits	2740
DSA	[FIPS 186-3] Functions: Signature Verification Key sizes: 2048 bits with SHA-256	839
RNG	ANSI X9.31-1998 using AES-256	1265
SHA	[FIPS 180-4] Functions: Digital Signature Verification within Boot Loader SHA sizes: SHA-256	2312
SHA	[FIPS 180-4] Functions: Hash only within Application SHA sizes: SHA-256	2311

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES Key Wrap/Unwrap	AES (Cert. #2740, key wrapping)
Non-SP 800-56A Compliant DH	[IG D.8] Diffie-Hellman (key agreement; key establishment methodology provides at least 112 bits of encryption strength)
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 64 bits per access. The NDRNG output is used to seed the FIPS Approved RNG by concatenating (128) 64 bit random numbers generated from the hardware NDRNG then hashing the resultant 8192 bit value with SHA-256.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 6 – Critical Security Parameters (CSPs)

CSP	Description / Usage
RNG-SEED	128-bit random value used for ANSI X9.31 RNG seed, updated upon crypto module power-up by concatenating (128) 64 bit random numbers generated from the hardware ND-RNG then hashing the resultant 8192 bit value with SHA256.
RNG-SEED-KEY	AES 256 seed key used for ANSI X9.31 RNG. This is created by concatenating (128) 64 bit random numbers generated from the hardware ND-RNG then hashing the resultant 8192 bit value with SHA256.
RNG-STATE	256-bit random value and 128 bit counter value.
DH-Private	Private component of the DH 2048 key pair. Also used for User authentication.
KEKs[1]	One or more AES 256 Key Encryption Keys used to wrap TEKs for transmission from Master to Slave units.
TEK	AES 256 Traffic Encryption Key. Also used for User authentication.

2.2 Public Keys

Table 7 – Public Keys

Key	Description / Usage
DSA FW-Load Public Key	Public component of a DSA key pair (2048- bit), used for signature verification of the firmware image loaded into the Module. Also used for CO authentication.
DH-Public	Public component of the DH 2048 key pair. Also used for User authentication.
Other Party's DH Public Keys	One or more of Other Party's DH 2048 keys. Also used for User authentication.

[1] The effective security strength is 112 bits, provided by the key establishment methodology.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles by using different authentication mechanisms. One CO authentication is allowed per module reset. Re-authentication is enforced when changing role from CO to User. Authentication for both CO and User are Identity based with CO identity being associated with Signature Certificate of the Application Firmware and User associated with D-H Private Key and TEK.

The Module supports a bypass capability. The Enable/Disable Bypass service is accessed only one time upon boot-up using a configuration setting in the Master. Power cycle of the module is required to access the Enable/Disable Bypass service again, at that time all CSPs are zeroized and previous authentications are cleared. The signing of Boot Loader and Application Firmware files to be loaded onto the crypto module shall be done at the factory by a signature officer responsible for insuring that the keys are protected from unauthorized disclosure. Additionally the signature office insures, no unauthorized modification or substitutions of keys are possible and that obscured feedback is utilized when creating the signature keys.

Table 8 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – This is the UIM boot loader module.	Identity-based	DSA 2048 with SHA-256 Verify
User	User – This is the FPG and the UIM after boot up.	Identity-based	1. D-H 2048 Mutual Authentication 2. AES 256 with TEK

3.2 Authentication Methods

DSA 2048 with SHA-256 Verify

The CO authentication method is DSA 2048 with SHA-256 Verify. This method was chosen to meet the requirements of FIPS-140-2. The CO authentication is only performed during boot-up and requires a power cycle of the crypto module to re-authenticate. The authentication only occurs once and only one authentication attempt is allowed.

D-H 2048 Mutual Authentication

This User authentication is Diffie-Hellman 2048 Mutual Authentication. This mutual authentication occurs between two stations over a satellite link. The rate of authentication is limited by satellite round trip communication time, at minimum .5 seconds. Please refer to Table 9 – Authentication Description, for more details regarding the probability of successful authentication.

AES 256 with TEK

This User authentication method is AES 256 with TEK. Please refer to Table 9 – Authentication Description, for more details regarding the probability of successful authentication.

Table 9 – Authentication Description

Method	Probability	Probability in One-Minute Period
DSA 2048 with SHA-256 verify	1/(2^112) which is < 1 / 1,000,000	For the CO role, only one authentication attempt is allowed per power cycle of the crypto module. Upon authentication failure the crypto module is put in a locked state and a log is made to indicate authentication failure. No other authentication attempts are allowed, a power cycle is required. It takes more than .5 seconds to reboot. Therefore attempts can occur in a one minute period, so 120/2^112 (which is < 1 / 100,000).
D-H 2048 Mutual Authentication	1/(2^112) which is < 1 / 1,000,000	The rate of authentication is limited by satellite round trip communication time, at minimum .5 seconds. If the DH Authentication attempt fails the module generates a high level log error and is un-registered by the Master. So no more than 60 authentication attempts can occur in a one minute period, so 60/2^112 (which is < 1 / 100,000).
AES 256 with TEK	1/(2^112) which is < 1 / 1,000,000	The rate of authentication is limited by satellite round trip communication time, at minimum .5 seconds. So no more than 120 authentication attempts can occur in a one minute period, so 120/2^112 (which is < 1 / 100,000). The strength of the AES-256 key is weakened because the key wrapping method only provides 112 bits of security.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 10 – Authenticated Services

Service	Description	CO	User
Boot Loader Firmware Load	Load Boot Loader Firmware to the module for DSA 2048 with SHA-256 verification. This is part of authentication of the CO.	X	
Application Firmware Load	Load Application Firmware to the module for DSA 2048 with SHA-256 verification. This is part of authentication of the CO.	X	
Enable/Disable Bypass	Send configuration of whether bypass is enabled or disabled. If bypass is disabled, further authenticated services will be performed by the User. If bypass is enabled, further services will be unauthenticated.	X	
Generate TEK	Generate the TEK using the Approved RNG.	X	
Non-Bypass - Frame Plan	Transmit Reference Burst. This is part of authentication of the User.		X
Non-Bypass - Request	Transmit Request Burst. This is part of authentication of the User.		X
Non-Bypass – Send/Receive TEK	Send or receive key wrapped TEK, depending on if the module is a master or slave.		X
Non-Bypass - Traffic	Encrypt and decrypt traffic with AES ECB 256.		X

Table 11 – Unauthenticated Services

Service	Description
Initialize (Self-test)	Power on initialization of the module, inclusive of power-on self-test functionality.
Power Off or Reset (Zeroize)	Powers off the Module, zeroizing all CSPs. On reset, reloads the image and performs power-on self-test and other initialization functions. RAM is cleared on power down, and thus all authentication data is destroyed and re-authentication must occur.
Show Status	Show various status outputs. E.g., version, bypass enabled/disabled, FIPS mode of operation, etc. This is obtained through low and high-level log files and SNMPv2 read only OIDs.
Send Files	Before authentication, application firmware and configuration files are sent to the module for verification.
Bypass - Frame Plan	Transmit Reference Burst unauthenticated if bypass is enabled.

Service	Description
Bypass - Request	Transmit Request Burst unauthenticated if bypass is enabled.
Bypass - Traffic	Send/receive plaintext data if bypass is enabled.

Table 12 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- U= Use: The module uses the CSP.
- E = Enter: The module receives the CSP (i.e., the CSP is entered into module).
- O = Output: The module outputs the CSP.
- Z = Zeroize: The module zeroizes the CSP.

Table 12 – CSP Access Rights within Services

Service	CSPs								
	RNG-SEED	RNG-SEED-KEY	RNG-STATE	DH-Private	KEK	TEK	DSA FW-Load Public Key	DH-Public	Other Party's DH Public Key
Boot Loader Firmware Load	GU	GU	GU				U		
Application Firmware Load	GU	GU	GU				U		
Enable/Disable Bypass									
Generate TEK						G			
Non-Bypass - Frame Plan						U			
Non-Bypass - Request				GU	GU	U		GUO	UE
Non-Bypass – Send/Receive TEK					U	UEO			
Non-Bypass - Traffic						U			
Initialize (Self-test)									
Power Off or Reset (Zeroize)	Z	Z	Z	Z	Z	Z		Z	Z
Show Status									
Send Files									
Bypass - Frame Plan									
Bypass - Request									
Bypass - Traffic									

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. The power on self-tests (POST) are available on demand by power cycling the module.

On power up or reset, the Module performs self-tests described in Table 13 below. All Tests must be completed successfully prior to any other use of cryptography by the Module. Therefore all data output is inhibited during Module self-tests. If one of the Tests fails, the Module enters the Diagnostic Mode (Diag. mode) error state and a low level log entry is generated. The Diag. Mode error state completely inhibits data output and requires a complete Module reset via power cycle to re-initialize.

Table 13 – Power Up Self-tests

Test Target	Description
Firmware Integrity	Boot Loader Firmware Integrity Test: 32 bit CRC
Firmware Integrity	Application Firmware Integrity Test: DSA 2048 signature verification
AES	KATs: Encryption, Decryption, Modes: ECB, Key sizes: 256 bits
AES Key Wrap	KATs: Wrap, Unwrap, Modes: ECB, Key sizes: 256 bits
DSA	KAT: Signature Verification, Key sizes: 2048 bits
RNG	KATs: ANSI X9.31-1998 using AES-256
SHA	KATs: SHA-256 within Boot Loader
SHA	KATs: SHA-256 within Application

Table 14 – Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
RNG	RNG Continuous Test performed when a random value is requested from the RNG.
Non-SP 800-56A Compliant DH	Pairwise Consistency Test performed on every DH key pair generation per FIPS IG 9.9.
Firmware Load	DSA 2048 signature verification performed when Boot Loader firmware is loaded.
Firmware Load	DSA 2048 signature verification performed when Application firmware is loaded.
Bypass Test	Exclusive Bypass Test performed.

Table 15 – Critical Function Tests

Test Target	Description
N/A	

5 Physical Security Policy

The module uses standard, production-quality IC, designed to meet commercial-grade specifications for power, temperature, reliability, shock and vibration. A hard, opaque potting material is applied to the top and bottom of the crypto module. The potting material protects against environmental of other physical damage. The potting provides tamper evidence to deter direct observation, probing, or manipulation of module components and is visibly opaque within the visible spectrum. Any attempt to remove the potting material shall result in a permanent change from a dark to light color. Additionally, the potting hardness assures that moderately aggressive force with hand tools shall not allow access to underlying circuitry.

Table 16 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, Opaque potting	Annually and Upon delivery, any time module is installed or removed or suspected of being tampered with.	Inspection of physical damage is detailed in our SKYWAN IDU7000 FIPS 140-2 Module - Delivery and Installation Procedure Guide

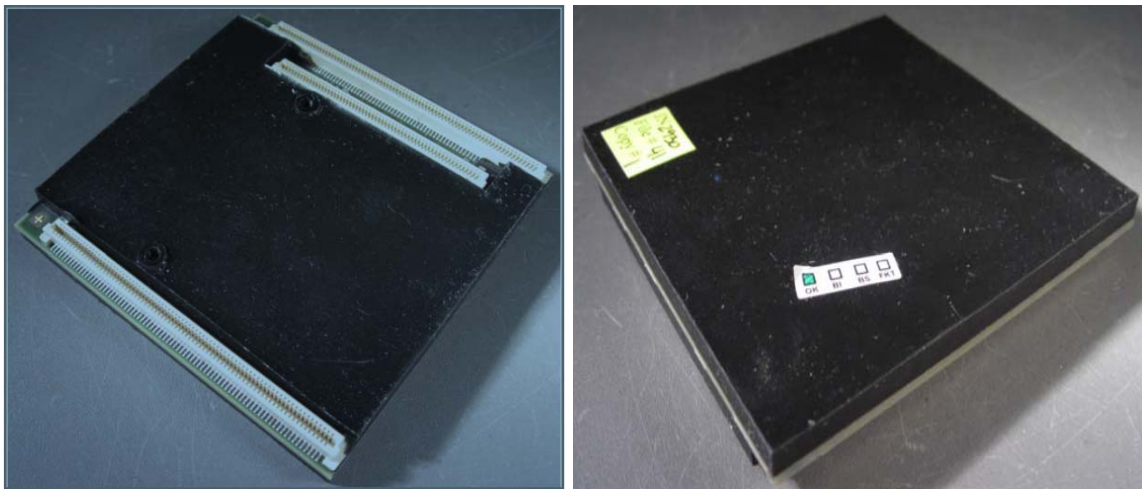

Figure 2 - Hard, opaque potting on crypto module

As seen in figure 2 above, there are a few visable traces and componants (see excluded components list below) that are not covered by the hard, opaque potting material. These traces and companantsare not security relevant and no malfunction or misuse of these components could lead to comprimising of CSPs or other sensitive materials. The excluded components are listed in Section 1.1.

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Module does not implement any mitigation of other attacks beyond those described in FIPS 140-2.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The module shall clear previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The operator shall be capable of commanding the module to perform the power up self-tests by cycling power or resetting the module.
4. Power up self-tests do not require any operator action.
5. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module ensures that the seed and seed key inputs to the Approved RNG are not equal.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not enter or output plaintext CSPs.
12. The module does not output intermediate key values.

9 References and Definitions

Table 17 – Acronyms and Definitions

Acronym	Definition
SIC DEMOD	Satellite Interface Controller Demodulator subsystem (satellite modem controller)
SoC	System on a Chip
Master	This is the Primary Satellite Network Modem with the primary crypto module
Slave	All other Satellite Modems, they perform DH Process with Master
BUM	Backup Master is the Slave Modem that can take over Master role if Master Fails (only one allowed per network)
TX/RX	Transmit/Receive over Satellite
Diag. Mode	Diagnostic mode: This is a frozen error state of the modem and crypto module.
UIM	User Interface Module of the satellite modem
FPG	Frame Plan Generator of the satellite modem
FPGA	Field Programmable Gate Array