Security Policy

for

Vertex Standard Cryptographic Module 001

Version 1.0.1

FIPS 140-2 Non-Proprietary

Revision History

Date	Revision	Description
10/16/2008	1.0.0	Initial Release
2/4/2009	1.0.1	2nd Release Section 3 Modes of Operation (encryption -> obfuscation) Section 8 Security Rules #13 added the following comments, "The module shall output status code 0x10 to indicate that it is in an error state.
2/12/2009	1.0.1	3rd Release Updated the Version number from "1.0.0" to "1.0.1" on Page 1

Table of Contents

Revision History 2
1. Module Overview 4
2. Security Level 6
3. Modes of Operation 7
Approved mode of operation 7
Non-Approved mode of operation 7
4. Ports and Interfaces 8
5. Identification and Authentication Policy 9
Assumption of roles 9
6. Access Control Policy 10
Roles and Services 10
Services - Purposes and Uses 11
Definition of Critical Security Parameters (CSPs) 12
Definition of CSPs Modes of Access 13
7. Operational Environment 13
8. Security Rules 14
9. Physical Security Policy 16
Physical Security Mechanisms 16
Operator Required Actions 16
10. Mitigation of Other Attacks Policy 16
11. References 17
12. Definitions and Acronyms 18

1. Module Overview

This Security Policy is prepared as one of the requirements of FIPS 140-2 validation. However, Vertex Standard Co., Ltd. intends other purposes also.
It allows entities to:

- Determine if the cryptographic module is implemented as stated in this Security Policy.
- Describe how the FIPS 140-2 requirements are actually implemented in the cryptographic module.

The Vertex Standard Cryptographic Module 001 (VSCM) is a cryptographic module (also processes digital data) that is to be incorporated into two-way digital radio products. These digital radios are for use in communication with other APCO Project 25 compatible devices. The VSCM consists of:

- Hardware Part Number 013790D
- Firmware Version 71.72

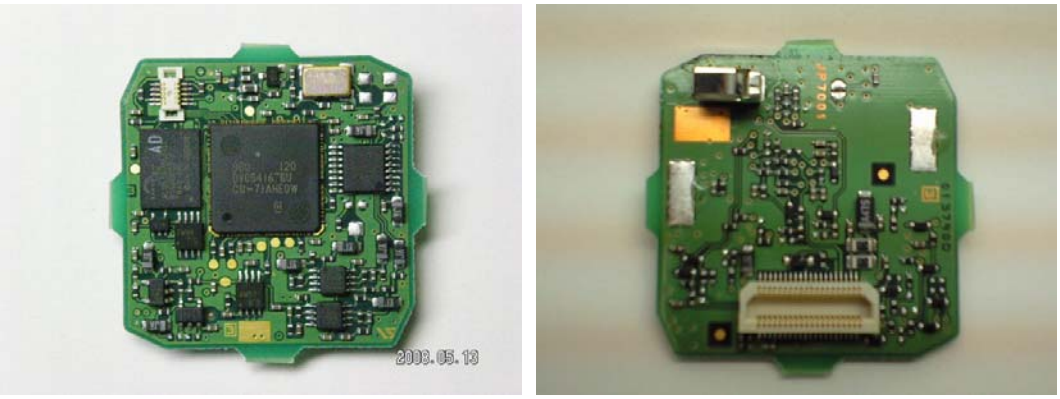
The VSCM is incorporated into the following models:

[Portable models]
- VX-P820 Series (VX-P821, VX-P824, VX-P829)
- VX-P870 Series (VX-P871, VX-P874, VX-P879)
- VX-P920 Series (VX-P921, VX-P924, VX-P929)
- VX-P970 Series (VX-P971, VX-P974, VX-P979)

[Mobile models]
- VX-7100 Series
- VX-7200 Series

The VSCM is a hardware cryptographic module targeted for FIPS 140-2 Security Level 1 overall. In FIPS 140-2 terms, the VSCM is a multi-chip embedded module and the physically contiguous cryptographic boundary as well as the logical boundary is defined

as the entire circuit board. All I/O is managed through the board-to-board connector that the VSCM employs. The following figure shows the VSCM and its defined cryptographic boundary.



top bottom

Figure 1 - Image of Cryptographic Module

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI / EMC	3
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved Algorithms

The VSCM supports both FIPS approved and non-FIPS approved algorithms. The module does not support a non-FIPS approved mode of operation, however upon access to the non-FIPS approved algorithm (DES), the module enters bypass mode and although obfuscation does take place, within the context of FIPS 140-2, any resulting output from the process is considered to be plaintext.

Table 2 - Approved Algorithms

AES	As defined in **FIPS PUB 197** with 256 bit keys. AES will support the following modes: ECB, OFB Cert. #813
SHS	As defined in **FIPS PUB 180-2** for generating message digests with 256 bit lengths. (SHA-256) Cert. #813 * This is used for internal functions only

Non-Approved Algorithms

The VSCM supports the following non-FIPS Approved algorithm as follows:

Table 3 - Non-Approved Algorithms

DES	As defined in **FIPS PUB 46-3** with 56 bit keys. DES will support the following mode : OFB
LFSR	Linear Feedback Shift Register, which is used for the generation of IV's to be used in OFB mode for encryption. * This algorithm at no time generates cryptographic keys.

The VSCM will send a signal to the radio and the user will be notified via the LED/LCD on the radio, which data processing mechanism is being used (e.g. AES or DES/no encryption bypass) Verification that the module is operating in a FIPS mode can be done by checking the part number on the bottom the VSCM to be '013790D' and the firmware version to be '71.72'. The module does not support a non-FIPS mode of operation.

4. Ports and Interfaces

The VSCM provides the following logical interfaces through the board-to-board connector (physical port):

- Data input
- Data output
- Control input
- Status Output

The VSCM receives power through the board-to-board connector from the radio system in which it resides on.

5. Identification and Authentication Policy

Assumption of roles

The VSCM supports two distinct operator roles (User and Cryptographic-Officer [C.O.]). The module does not support operator authentication or a maintenance role. The operator assumes a given role by utilizing the services that the module provides.

Table 4 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	N/A	N/A
C.O.	N/A	N/A

Table 5 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
N/A	N/A

6. Access Control Policy

Roles and Services

Table 6 - Services Authorized for Roles

Role	Authorized Services
User: The entity that has access to functions supported by the cryptographic module. This role ***implicitly*** selected by the operator by performing the services associated with this role.	• AES • DES (FIPS Approved Bypass mode) • No Encryption Bypass (FIPS Approved Bypass mode)
Cryptographic-Officer: The entity is responsible for key entry into the module. This role is ***implicitly*** selected when performing these services.	• Key Entry • Power-Up Self-tests • Zeroization • Show Status

Services - Purposes and Uses

Table 7 - Service names, purposes, and uses

Service Name	Purpose and Use
AES	Allows Users to encrypt / decrypt various data. This is also used for key wrapping/unwrapping.
DES (FIPS Approved Bypass mode)	Allows Users to encrypt / decrypt various data (Data encrypted using the DES algorithm is considered to be plaintext.)
No Encryption Bypass	Allows Users to process various data without encryption
Power-up Self tests	Allows CO to perform power-up self tests (This service can be obtained by power-cycling the module)
Show Status	Allows CO to determine if the module is functioning properly.
Key Entry	Allows CO to enter cryptographic keys into the module
Zeroization	Zeroization of cryptographic keys and CSPs within the module

Definition of Critical Security Parameters (CSPs)

The following **CSPs** are contained in the module:

- **CKEK (AES 256 bit key):**
  Used to decrypt the encrypted KEK that is input into the module in ECB mode. This key is pre-input into the module during the manufacturing process.
- **KEK (AES 256 bit key):**
  Used to decrypt the encrypted TEKs that are input into the module in ECB mode. This key is input into the module in encrypted form.
- **TEK (AES 256 bit key):**
  Used for encryption and decryption of various data in OFB mode. This key is input into the module in encrypted form.

* The CKEK is embedded within the module.

Definition of CSPs Modes of Access

Table 8 defines the relationship between access to **CSP**s and the different module services. The modes of access shown in the table are defined as follows:

Write **(*e*) :** a cryptographic key is written into the module's memory.
Read **(*u*) :** a cryptographic key is used to perform cryptographic operations within its corresponding service (as described in Section 3 of this document).
Output **(*o*) :** a cryptographic key is output from the module.
Zeroize **(*z*) :** a cryptographic key is destroyed.

Table 8 - CSP Access Rights within Services

Role		Service	CSP Access Operations		
C.O.	**User**		**CKEK**	**KEK**	**TEK**
	X	AES			***u***
	X	DES			
	X	No Enc. Byp.			
X		Power-up			
X		Key Entry	***u***	***e,u,z***	***e***
X		Show Status			
X		Zeroization	***z***		***z***

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable since the VSCM operates on a non-modifiable operational environment.

8. Security Rules

The VSCM's design corresponds to the VSCM's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Security Level 1 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 does not support user authentication.
3. Cryptographic keys are entered electronically in encrypted form.
4. The module does not support a Non-FIPS Approved mode of operation.
5. The module supports an exclusive bypass mode in which data passes through the module without AES encryption. (Data that is encrypted using DES is considered to be plaintext for purposes of FIPS 140-2)
6. The module performs 2 internal independent actions prior to entering bypass mode.
7. The module performs a conditional bypass test as per FIPS 140-2 §4.9.2 for the transition out of bypass mode.
8. The module does not support the updating of its firmware components.
9. The module shall not output cryptographic keys at any time.
10. The module shall not output CSPs at any time.
11. The cryptographic module shall perform the following tests without any operator actions:
    A. Power up Self-Tests:
        (1) Firmware Integrity Test (SHA-256 verification)
        (2) Cryptographic algorithm tests:
            a. AES Known Answer Test
            b. SHA-256 Known Answer Test
    B. Conditional Self-Tests:
        (1) Exclusive Bypass test
            – performed when the module enters/exits bypass mode
        (2) Continuous Random Number Generator Test
            – performed each time the LFSR is used.
12. If the operator wishes to perform the power up self-tests on demand, he/she should power cycle the module. i.e., the radio system in which the VSCM is being used

should be re-started.

13. If the module enters an error state due to the failing of self-tests, the module shall be returned to the vendor. . The module shall output status code 0x10 to indicate that it is in an error state.
14. Data output shall be inhibited during self-tests, zeroization, and error states.
15. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
16. The module shall not support concurrent operators as a Security Level 1 module.
17. The module shall inhibit cryptographic operations and data output while in all error states.

9. Physical Security Policy

Physical Security Mechanisms

The VSCM is intended to meet the FIPS 140-2 physical security requirements for Level 1. To meet these requirements the VSCM multi-chip embedded module includes the following mechanisms:

- Use of production grade components.

Operator Required Actions

There are no operator required actions as the module is intended to meet Level 1.

Table 9 – 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 module has ***not*** been designed to mitigate specific attacks outside the scope of FIPS 140-2.

Table 10 – Mitigation of Other Attacks

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

11. References

- National Institute of Standards and Technology, “FIPS PUB 140-2, Security Requirements for Cryptographic Modules”, May 25, 2001
- National Institute of Standards and Technology, “Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. Draft”, March 24, 2004
- National Institute of Standards and Technology, “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”, September 22, 2004.
- National Institute of Standards and Technology, “FIPS PUB 197, Advanced Encryption Standard (AES)”, November 26, 2001
- National Institute of Standards and Technology, “FIPS PUB 180-2, Secure Hash Standard (SHS)”, August 1, 2002
- National Institute of Standard and Technology, “FIPS PUB 46-3, Data Encryption Standard (DES)”, October 25, 1999
- TIA/EIA Standard, “102.AAAA-A , Project 25 DES Encryption Protocol”, January 23, 2001
- TIA/EIA Standard, “102.AAAD, Block Encryption Protocol”, June 13, 2002

12. Definitions and Acronyms

Table 11 – Definitions and Acronyms

APCO	Association of Public-Safety communications Officials-International
AES	Advanced Encryption Standard
DES	Data Encryption Standard
LFSR	Linear Feedback Shift Register
SHS	Secure Hash Standard – the message digest will be 160, 224, 256, 384, or 512 bits (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512).
VSCM	Vertex Standard Cryptographic Module 001