Security Policy
For The
Embeddable Security System (ES-1200)

Document No.: 1174943, Rev. 002
23 October 2013

Prepared By:

ViaSat Inc.
6155 El Camino Real
Carlsbad, California 92009

Revision Record

Revision	Rationale	Release Date	Affected Pages
001	Initial Release	15 August 2013	All
002	Update algorithm cert & table 1	23 October 2013	Page 2

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Security Policy

The ViaSat Embeddable Security System (ES-1200) (Hardware P/N 1174941, Rev. 001; Firmware Version 1.0.7) is a low cost, size, weight & power, programmable multi-chip embedded cryptographic module. It provides encryption and decryption services, plaintext bypass, key management, and PIN-based access control. The ES-1200 is intended for use in environments where FIPS 140-2 Level 2 cryptographic products are required. Typical applications are military Transmission Security (TRANSEC), Communications Security (COMSEC), and Data-at-Rest (DAR) using Suite B cryptography. The cryptographic boundary of the module is the entirety of the PCB, including its partial tamper resistant opaque coating (both sides), with the plastic cap and tamper label (primary side).

Figure 1 and Figure 2 show the ES-1200 and its cryptographic boundary.

Figure 1 - ES-1200 (Primary Side)

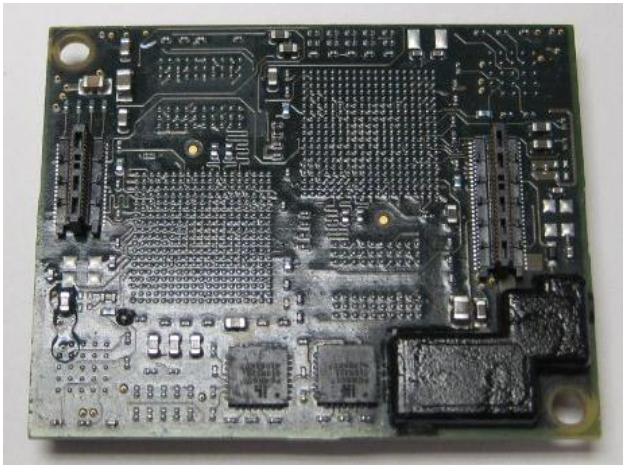

Figure 2 - ES-1200 (Secondary Side)

1.1 Security Level

The ES-1200 meets the overall requirements applicable to Level 2 security of FIPS 140-2. Table 1 specifies the levels met for specific FIPS 140-2 areas.

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	2
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.2 Modes of Operation

The ES-1200 runs strictly in one FIPS Approved mode of operation. The ES-1200 leaves the factory in a FIPS Approved mode of operation and does not contain a Non-FIPS Approved mode of operation. The operator invokes the FIPS Approved mode of operation simply by powering on the ES-1200. Upon first-time start-up or after a Zeroize All the user is required to create a new PIN and role to enter the FIPS Approved mode of operation.

The ES-1200 supports the following sub-modes of operation:

- Ciphertext Mode: Encrypt/Decrypt user traffic. While in Ciphertext mode, the ES-1200 supports a plaintext override function that allows for user traffic to be received unencrypted.
- Plaintext Mode: Allow user traffic to flow through the ES-1200 unencrypted.

The ES-1200 supports the following FIPS Approved and FIPS allowed algorithms:

- AES ECB mode with 256 bit keys for AES key wrap (used within processor) [Cert. # 2633]
- SP800-38A AES CTR modes with 256 bit keys for encryption (used within processor for random number generation) [Cert. # 2633]
- SP800-38A AES CTR modes with 256 bit keys for encryption (used within FPGA for traffic processing) [Cert. # 2635]
- SP800-38A AES ECB modes with 256 bit keys for encryption (used within FPGA for traffic processing) [Cert. # 2634]
- SP800-90 CTR_DRBG using SP800-38A AES CTR mode with 256-bit key for generating key material, initial counter and nonces [Cert. # 406]
- SHA-512 for hashing [Cert. # 2207]

1.3 Ports and Interfaces

The ES-1200 provides the following physical ports and logical interfaces:

Table 2 - Physical Ports and Logical Interfaces

Physical Port	Logical Interfaces Supported
Power Port	N/A
Plaintext Serial Peripheral Interface (SPI)	• Control Input: Commands received on virtual channel 0 • Status Output: Status sent on virtual channel 0 • Data Input: Messages received on virtual channel 1 – N • Data Output: Messages sent out on virtual channel 1 – N
Ciphertext Serial Peripheral Interface (SPI)	• Control Input: Commands received on virtual channel 0 • Status Output: Status sent on virtual channel 0 • Data Input: Messages received on virtual channel 1 – N • Data Output: Messages sent out on virtual channel 1 – N

2 Identification and Authentication Policy

The ES-1200 supports three distinct operator roles. The module enforces the separation of roles using role-based operator authentication. Table 3 lists the supported operator roles along with their required identification and authentication techniques. Table 4 outlines each authentication mechanism and the associated strengths.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication	Password authentication
Crypto-Officer (Admin)	Role-based operator authentication	Password authentication
Crypto-Officer+User	Role-based operator authentication	Password authentication

Table 4 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
PIN/Password	A password consists of 6 hex digits (i.e. 24 bits). The probability that a random attempt will succeed or a false acceptance will occur is 1/16777216 which is less than 1/1,000,000. Entering the incorrect pin 5 times consecutively will cause an access control zeroize event and reset the module. The probability of successfully authenticating to the module within one minute is 5/16777216 which is less than 1/100,000. The password length is restricted via the module itself.

3 Access Control Policy

3.1 Roles and Services

Table 5 lists each operator role and the services authorized for each role. All operators assuming an authenticated role (i.e. User, Crypto-Officer, and Crypto-Officer+User) must provide a valid PIN for authentication prior to assuming that role.

Table 5 - Services Authorized for Roles

Roles				Authorized Services
Unauthenticated User	User	Crypto-Officer (Admin)	Crypto-Officer + User	
	X		X	**Query Statistics/Key/Service Info** **Create/Delete Virtual Circuits (for services)** **Change Modes** **Fill Key** **Delete Key** **Encrypt/Decrypt user traffic** **Bypass user traffic** **Bypass control/status data**
		X	X	**List Users** **Update User** **Delete User**
X[1]				**Create User** **Authenticate User**
X	X		X	**Request Status** **Clear Status** **Initiated BIT** **Version Info**
X[2]				**Zeroize All:** Zeroize all volatile and non-volatile CSPs and reset hardware **Access Control Zeroize:** Zeroize all volatile CSPs and reset hardware **Reset via Discrete** **Power On/Off and POST** **View Status via Discrete**

3.2 Definition of Critical Security Parameters (CSPs)

The following Critical Security Parameters (CSPs) are used in the module:

- **Master Local Unique Key (MLUK):** Generated internally using random data from CTR_DRBG (SP800-90 compliant).
- **Traffic Encryption Key (TEK)**: 256 bit AES key. Entered via control interface. Used

[1] These services are explicitly disallowed by authenticated operators in any role.

[2] These services are available to any operator whether authenticated or unauthenticated.

with AES-CTR to protect user traffic.

- **Master Key Encryption Key (MKEK):** 256-bit key. Internally generated using random data from CTR_DRBG (SP 800-90 compliant).
- **DRBG AES Key**: 256 bit entropy source input as AES key for the SP 800-90 DRBG. Prior to generating random bits, the DRBG AES key must be generated.
- **DRBG AES IV**: 128 bit entropy source input as AES Initialization Vector for the SP 800-90 DRBG. Prior to generating random bits, the DRBG AES IV must be generated.
- **Password/PIN**: 24-bit password/PIN (i.e. 6 hexadecimal characters). Entered via control interface. Used to authenticate the operator and provide services applicable to the user's role.
- **Cache Protection Value:** 2048 byte value. Value is internally generated from CTR_DRBG (SP 800-90 compliant) upon bootup.

3.3 Definition of Public Keys

None

3.4 Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The types of access used in the table are Generate (G), Read memory (R), Write to volatile memory (WV), Write to non-volatile memory (WNV), Zeroize (ZV), and Zeroize non-volatile memory (ZNV). No CSP is ever permitted to leave the security boundary of the cryptographic module once entered.

Table 6 - CSP Access Rights within Services

Services	Master Local Unique Key (MLUK)	Traffic Encryption Key (TEK)	Master Key Encryption Key (MKEK)	DRBG AES Key & IV	Password/PIN	Cache Protection Value
Query Statistics/Key/Service/Version Info Request/Clear Status View Status via Discrete	N/A	R	N/A	N/A	N/A	N/A
Create Virtual Circuits (for services)	R	R/WV	N/A	R/WV	N/A	R
Delete Virtual Circuits (for services)	N/A	ZV	N/A	N/A	N/A	N/A
Change Modes	N/A	ZV	N/A	N/A	N/A	N/A
Fill Key	R	WV/WNV	N/A	N/A	N/A	R
Delete Key	N/A	ZV/ZNV	N/A	N/A	N/A	N/A
Encrypt/Decrypt User Traffic Initiated BIT	N/A	R	N/A	N/A	N/A	R
Bypass User Traffic Bypass Control/Status Data	N/A	N/A	N/A	N/A	N/A	N/A
List Users	N/A	N/A	N/A	N/A	N/A	N/A
Update User	R/WV/WNV/ZV/ZNV	N/A	R	N/A	R/WV	R
Delete User	ZV/ZNV	ZV/ZNV	N/A	N/A	N/A	N/A
Create User	G/WNV	N/A	GV/WNV	RV/WV	RV/WV	R
Authenticate User	R	N/A	R	N/A	R/WV	R
Self Tests Power On/Off Reset via Discrete	R	R	R	R/WV	N/A	R/WV
Zeroize All	ZV/ZNV	ZV/ZNV	ZV/ZNV	ZV	ZV	ZV
Access Control Zeroize	ZV	ZV	ZV	ZV	ZV	ZV

4 Physical Security Policy

4.1 Physical Security Mechanisms

The ES-1200 multi-chip embedded cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque tamper resistant coating (i.e. potting material)
- Production-grade cap, adhesive and anti-tamper labels

The tamper resistant potting material, cap, adhesive and anti-tamper label are applied during the manufacturing process.

4.2 Operator Required Actions

The operator is required to periodically inspect the module for evidence of tamper. Table 7 outlines the recommendations for inspecting/testing physical security mechanisms of the module.

Table 7 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Resistant Opaque Coating located on both primary and secondary sides	As specified per end user policy	Visually inspect the coating for tears, rips, dissolved coating and other signs of malice.
Cap located on primary side	As specified per end user policy	Visually inspect the cap for tears, rips, dissolved coating and other signs of malice.
Cap adhesive on primary side	As specified per end user policy	Visually inspect the adhesive material between the cap and circuit board for scratches, divots, missing material and other signs of malice.
Circular Anti-tamper label on primary side	As specified per end user policy	Visually inspect the circular anti-tamper label for tears, rips, and any indication of removal. The label has a continuous foil surface that will tear and leave behind small opens in the foil surface if removed.

Figure 3 depicts the ES-1200 tamper resistant opaque coating on both the primary and secondary sides of the unit.

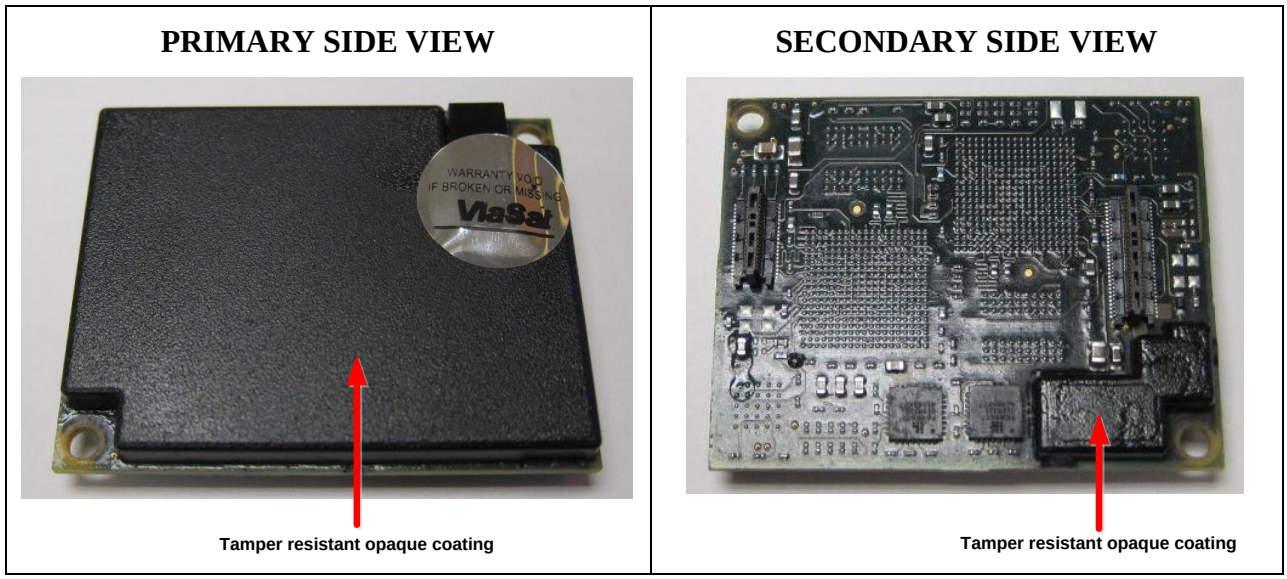

Figure 3 - Tamper Resistant Opaque Coating

Figure 4 depicts the ES-1200 cap (partially covered by the circular anti-tamper label), cap adhesive located on two sides of the cap as shown in white in both View A and View B, and circular anti-tamper label.

VIEW A

VIEW B

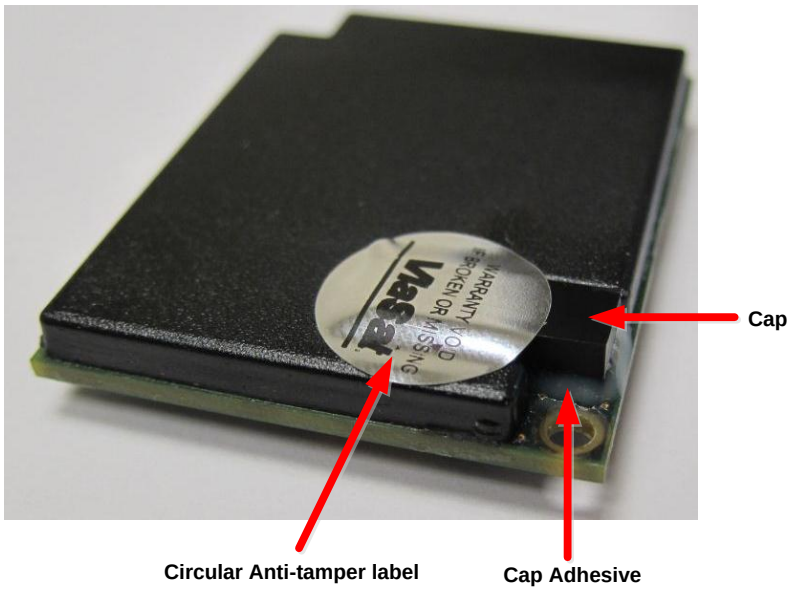

Figure 4 - Anti-tamper Cap, Adhesive, and Circular Label

5 Security Rules

The ES-1200's design corresponds to the following security rules. The security rules are enforced by the module in order to comply with the requirements for FIPS 140-2 Level 2.

1. The cryptographic module shall support defined roles with a defined set of corresponding services. The defined roles shall be: User, Crypto-Officer, and User+Crypto-Officer.
2. The cryptographic module shall allow on first-time start-up or after a Zeroize All any user to create a new PIN and assign it a role. The user shall be required to create a new PIN and role upon first-time start-up or after a Zeroize All to enter the FIPS Approved mode of operation.
3. The cryptographic module shall provide role-based authentication for all security relevant services; re-authentication shall be required to change roles.
4. When an operator has not been authenticated to a valid role, the operator shall not have access to any cryptographic services.
5. The cryptographic module shall not support a maintenance role or maintenance interface.
6. The purpose, function, service inputs, and service outputs performed by each role shall be defined and appropriately restricted.
7. The cryptographic module shall not support the output of plaintext CSPs.
8. The cryptographic module design shall ensure that unauthenticated services do not provide the ability to modify, disclose, or substitute any module CSPs, use approved security functions, or otherwise affect module security.
9. The module shall not support concurrent operators.
10. The module shall support a bypass capability and enable it upon receipt of (i) request to transition to a plaintext mode and (ii) request to create a plaintext circuit.
11. Re-authentication shall be required upon power cycling the module.
12. The cryptographic module's finite state machine shall provide a clear description of all states and corresponding state transitions. The design of the cryptographic module shall disallow the ability to simultaneously occupy more than one state at a time.
13. The cryptographic module's physically contiguous cryptographic boundary shall be defined including all module components and connections (ports), information flows, processing, and input/output data. Visible vendor-defined non-security relevant circuitry shall be argued for exclusion from the cryptographic boundary.
14. All cryptographic module data output shall be inhibited when the module is in an error state or during self-tests.
15. Data output shall be logically disconnected from the processes performing key generation and zeroization.
16. All physical ports and logical interfaces shall be defined; the cryptographic module shall be able to distinguish between data and control for input and data and status for output. In addition, the cryptographic module shall support a power interface.

17. All of the implemented integrated circuits shall be standard quality, production-grade components.
18. The cryptographic module shall contain an opaque tamper resistant potting material.
19. CSPs shall be protected against unauthorized disclosure, modification, and substitution. Critical settings shall be protected against unauthorized modification and substitution.
20. The cryptographic module shall support key generation using an Approved DRBG listed in FIPS PUB 140-2 Annex C.
21. The cryptographic module shall ensure that the inputs to the approved DRBGs meet the requirements of SP 800-90.
22. The cryptographic module shall not support any key establishment techniques.
23. The cryptographic module shall provide the ability to zeroize all plaintext CSPs.
24. Power-up self-tests shall not require operator actions. The cryptographic module shall provide an indicator upon successful self-test completion as follows:
    a. Alarm Discrete de-asserted
25. The cryptographic module shall enter an error state upon failure of any self-test and shall provide an indicator upon failure as follows:
    a. Alarm Discrete asserted
26. Upon entering an error state, the cryptographic module shall inhibit all data outputs, inhibit cryptographic operations, and shall provide error status. The status output shall not contain any CSPs or other sensitive information that could be used to compromise the cryptographic module.
27. The cryptographic module shall perform the following self-tests:
    a. <u>Power Up Self-Tests:</u>
        i. Cryptographic Algorithm Tests:
            (1) AES ECB Encrypt/Decrypt KAT (Known Answer Test) FW
            (2) AES ECB Encrypt KAT PL
            (3) SP 800-90 DRBG KAT
            (4) Crypto Bypass KAT
            (5) SHA-512 KAT
        ii. Firmware Integrity Test: Performed on all executable code using a 32 bit Error Detection Code (EDC)
    b. <u>Conditional Self-Tests:</u>
        i. SP 800-90 DRBG Continuous Test
        ii. NDRNG Entropy source Continuous Test
        iii. Bypass Test when changing between Ciphertext and Plaintext modes
    c. Critical Functions Tests:

i. SDRAM Test: Walking Zeros, Walking Ones, Power of Two

28. If a non FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

6 Mitigation of Other Attacks Policy

The ES-1200 has not been designed to mitigate any other attacks outside of the scope of FIPS 140-2.

7 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the ES-1200 does not contain a modifiable operational environment.

8 References

FIPS PUB 140-2; National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, December 3, 2002

DTR for FIPS 140-2; National Institute of Standards and Technology, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules (Draft),* January 4, 2011

IG for FIPS 140-2; National Institute of Standards and Technology, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, July 15, 2011

SP 800-90; National Institute of Standards and Technology, *NIST Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised),* March 2007

FIPS PUB 180-3; National Institute of Standards and Technology, *Secure Hash Standard, Federal Information Processing Standards Publication 180-3 Secure Hash Standard,* October 2008

FIPS PUB 197; National Institute of Standards and Technology, *Federal Information Processing Standards Publication 197 Advanced Encryption Standard (AES)*, March 6, 2002

SP800-38A; National Institute of Standards and Technology, *NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation*, 2001

9 Definitions and Acronyms

AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
BIT	Built In Test
CCITT	Consultative Committee on International Telephone and Telegraph
COMSEC	Communications Security
CRC	Cyclical Redundancy Check
CSP	Critical Security Parameters
CT	Ciphertext
CTR	Counter
DoD	Department of Defense
DRBG	Deterministic Random Bit Generator
DTR	Derived Test Requirements
ECB	Electronic Cook Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HDL	Hardware Description Language
ICD	Interface Control Document
IDD	Interface Design Document
IG	Implementation Guide
IV	Initialization Vector
KEK	Key Encryption Key
MKEK	Master KEK
MLUK	Master Local Unique Key
MTBF	Mean Time Between Failure
NIST	National Institute of Standards and Technology
PCB	Printed Circuit Board
POST	Power On Self Test
PT	Plaintext
RNG	Random Number Generator
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SP	Special Publication
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
TEK	Traffic Encryption Key
TRANSEC	Transmission Security