Vidyo, Inc.

Cryptographic Security Kernel

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

Prepared for:

Vidyo, Inc.
433 Hackensack Ave., 6th Floor
Hackensack, NJ 07601
United States of America

Phone: +1 (866) 998-4396
Email: info@vidyo.com
http://www.vidyo.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
Unites States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cryptographic Security Kernel (Software Version: 1.0) from Vidyo, Inc. This Security Policy describes how the Cryptographic Security Kernel meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in the FIPS-Approved mode of operation, its only mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The Cryptographic Security Kernel is referred to in this document as Vidyo CSK, crypto-module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Vidyo website (http://www.vidyo.com) contains information on the full line of products from Vidyo.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Vidyo. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Vidyo and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Vidyo.

2 Cryptographic Security Kernel

2.1 Overview

Vidyo, Inc. was founded in 2005 to create superior IP[1] video conferencing technology and products. Vidyo's patented VidyoRouter™ architecture introduces Adaptive Video Layering, which dynamically optimizes the video for each endpoint by leveraging H.264 Scalable Video Coding (SVC)-based compression technology and Vidyo's Intellectual Property. The VidyoRouter™ architecture delivers low latency, High Definition video conferencing over general data networks and the Internet, using off-the-shelf devices. Vidyo's architecture dynamically optimizes video quality to the network and to the capabilities of individual endpoint devices in order to deliver telepresence-quality experiences for each participant.

Vidyo has been able to pack all of this technology into one, easily deployable Software Development Kit (SDK). The SDK, which exists in all of Vidyo's applications and products, consists of multiple libraries that assist Vidyo's proprietary technology. One important library, centrally located within the SDK, is the Cryptographic Security Kernel, or CSK. The Vidyo CSK offers a secure random number generator conforming to NIST SP 800-90 regulations, message authentication, and secure encryption and decryption. The CSK can be deployed in both server-side and client-side applications.

The primary use of the CSK is to provide cryptographic functionality to the SDK. The SDK takes advantage of the Vidyo CSK library to create master keys, which can then be used to create a secure session key. The SDK is available to any third-party vendors that are interested in integrating Vidyo's AVLA technology into their own products.

Figure 1 shows a sample deployment of Vidyo's products, each executing the Cryptographic Security Kernel to provide secure video and data transmission.

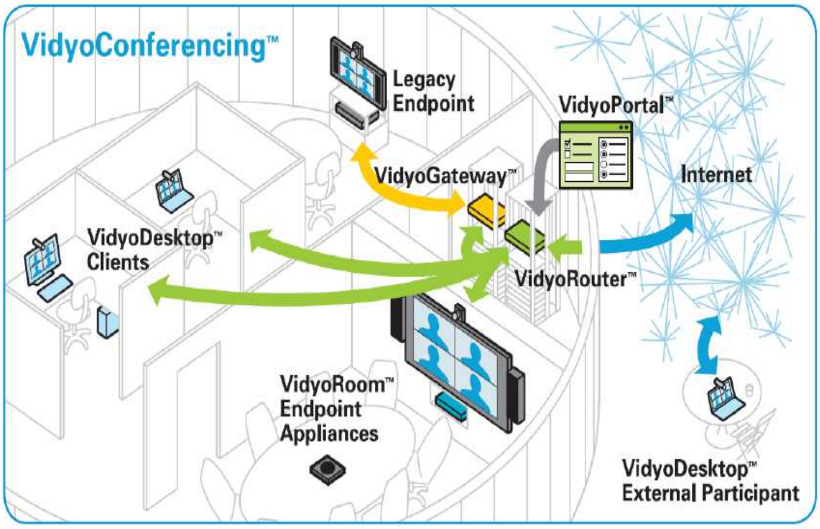

Figure 1 – Vidyo Product Deployment

The Cryptographic Security Kernel is validated at Level 1 FIPS 140-2 Section levels, show in Table 1 below.

[1] IP – Internet Protocol

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[2]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Vidyo Cryptographic Security Kernel is a software module with a multi-chip standalone embodiment. The overall security level of the module is 1. The following sections will define the physical and logical boundary of the module.

2.2.1 Physical Cryptographic Boundary

As a software cryptographic module, the module must rely on the physical characteristics of the host system to provide a physical cryptographic boundary. The physical boundary of the cryptographic module is defined by the hard enclosure around the host system on which it runs. The module supports the physical interfaces of a GPC, including the integrated circuits of the system board, the CPU[3], network adapters, RAM[4], hard disk, device case, power supply, and fans. Other devices may be attached to the GPC, such as a display monitor, keyboard, mouse, printer, or storage media. See Figure 2 for a standard GPC block diagram.

[2] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[3] CPU – Central Processing Unit
[4] RAM – Random Access Memory

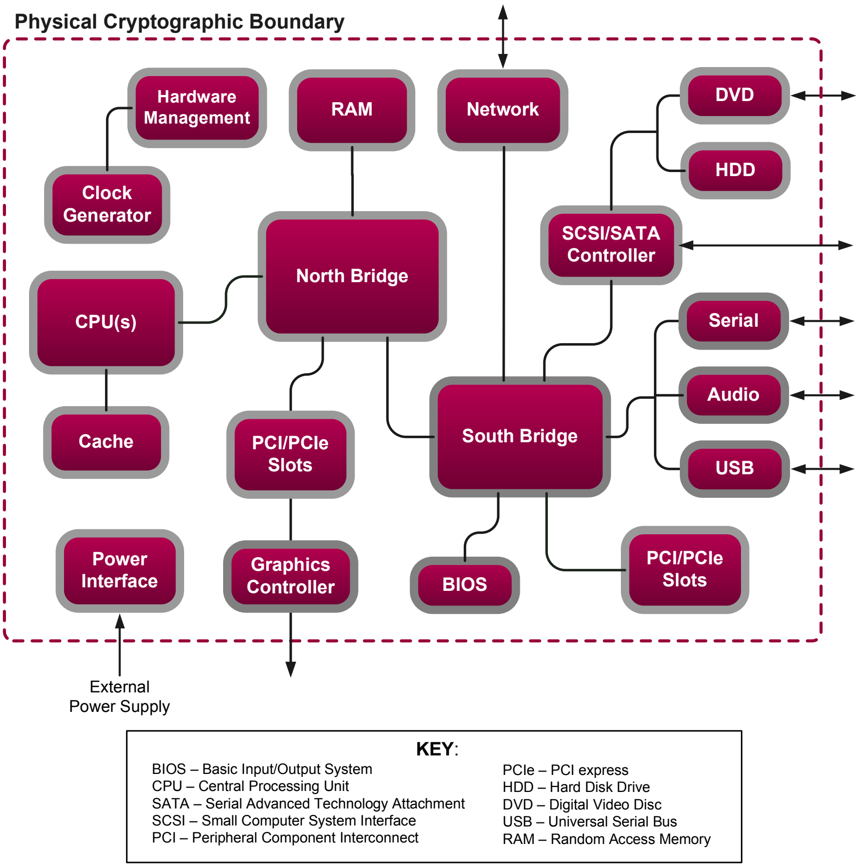

Figure 2 – Standard GPC Block Diagram

2.2.2 Logical Cryptographic Boundary

The logical cryptographic boundary of the Vidyo CSK consists of a compiled version of the Cryptographic Security Kernel. Figure 3 shows a logical block diagram of the module executing in memory and its interactions with surrounding software components, as well as the module’s logical cryptographic boundary. The module’s services are designed to be called by Vidyo’s SDK.

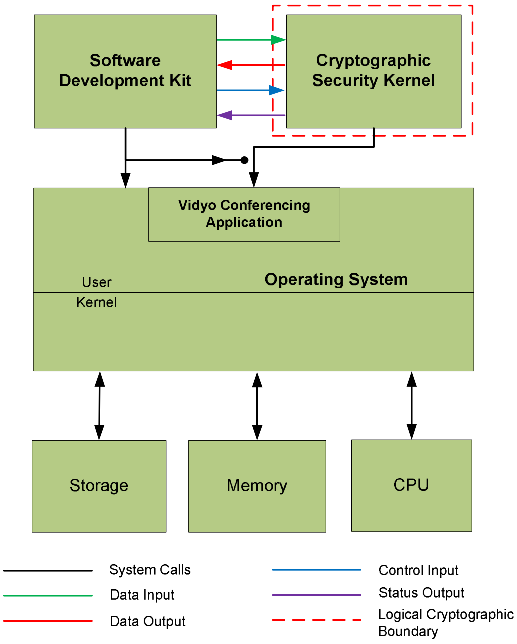

Figure 3 – Vidyo CSK Logical Cryptographic Boundary

2.3 Module Interfaces

The module's logical interfaces exist at a low level in the software as an Application Programming Interface (API). Both the API and physical interfaces can be categorized into following interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output
- Power input

As a software module, the module has no physical characteristics. Thus, the module's manual controls, physical indicators, and physical and electrical characteristics are those of the host platform. A mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module interfaces can be found in Table 2 below.

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS Interface	Physical Interface	Module Interface (API)
Data Input	USB[5] ports (keyboard, mouse, data), network ports, serial ports, SCSI[6]/SATA[7] ports, DVD[8] drive	The API calls that accept input data for processing through their arguments.
Data Output	Monitor, USB ports, network ports, serial ports, SCSI/SATA ports, audio ports, DVD drive	The API calls that return by means of their return codes or arguments generated or processed data back to the caller.
Control Input	USB ports (keyboard, mouse), network ports, serial ports, power switch	The API calls that are used to initialize and control the operation of the module.
Status Output	Monitor, network ports, serial ports	Return values for API calls.

2.4 Roles and Services

The Cryptographic Security Kernel supports the following two roles for operators, as required by FIPS 140-2: Crypto Officer (CO) role and User role. The CO and User both have access to the same cryptographic operations and other approved security functions such as asymmetric encryption or decryption, hashing, random number generation, and message authentication functions. Both roles are implicitly assumed, and operators may assume both roles simultaneously. Table 3 lists the services available to both the CO and the User.

Note 1: Table 3 uses the following definitions for "CSP[9] and Type of Access":

> ***R – Read:*** *The plaintext CSP is read by the service.*
> ***W – Write:*** *The CSP is established, generated, modified**,** or zeroized by the service.*
> ***X – Execute:*** *The CSP is used within an Approved (or allowed) security function or authentication mechanism.*

Note 2: Input parameters of an API call that are not specifically a signature, hash, message, plaintext, ciphertext, or a key are NOT itemized in the "Input" column, since it is assumed that most API calls will have such parameters.

[5] USB – Universal Serial Bus
[6] SCSI – Small Computer System Interface
[7] SATA – Serial Advanced Technology Attachment
[8] DVD – Digital Video Disc
[9] CSP – Critical Security Parameter

Table 3 – Crypto Officer and User Services

Service	Description	Input	Output	CSP and Type of Access
LmiAesEncKeySchedConstruct	Construct an AES encryption key schedule from a key	Key, API Call Parameters	Data, Status Message	AES Key – R
LmiAesEncKeySchedDestruct	Destruct an AES encryption key schedule, zeroing its associated memory	Data, API Call Parameters	None	AES Key – W
LmiAesEncKeySchedEncryptCtr	Use an AES encryption key schedule to perform counter-mode encryption on a block of memory	Plaintext or Ciphertext, Counter Value, Data, API Parameters	Ciphertext or Plaintext, Status Message	AES Key – X
LmiHmacSha1CtxConstruct	Construct an HMAC SHA-1 context with a specified key	Key, API Call Parameters	Data, Status Message	HMAC Key – RX
LmiHmacSha1CtxDestruct	Destruct an HMAC SHA-1 context, erasing its associated memory	Data, API Call Parameters	None	HMAC Key – W
LmiHmacSha1CtxFinal	Finalize an HMAC SHA-1 context and retrieve its authentication tag	Data, API Call Parameters	Data, Hash, Status Message	HMAC Key – X
LmiHmacSha1CtxInit	Reinitialize an HMAC SHA-1 context to its state as it was immediately after being constructed	Data, API Call Parameters	Data, Status Message	HMAC Key – X
LmiHmacSha1CtxUpdate	Update an HMAC SHA-1 context with additional message data	Message, Data, API Call Parameters	Data, Status Message	HMAC Key – X
LmiSecureRandomGeneratorConstruct	Construct (instantiate) a DRBG	API Call Parameters	Data, Status Message	DRBG “V” Value – W DRBG “Key” Value – W
LmiSecureRandomGeneratorDestruct	Destruct (uninstantiate) a DRBG	Data, API Call Parameters	None	DRBG “V” Value – W DRBG “Key” Value – W

Service	Description	Input	Output	CSP and Type of Access
LmiSecureRandomGeneratorGenerate	Generate random bytes	Data, API Call Parameters	Data, Random Number, Status Message	DRBG "V" Value – XW DRBG "Key" Value – XW DRBG Seed – X
LmiSecureRandomGeneratorGenerateEx	Generate random bytes	Data, Seed, API Call Parameters	Data, Random Number, Status Message	DRBG "V" Value – XW DRBG "Key" Value – XW DRBG Seed – X
LmiSecureRandomGeneratorHadCatastrophicError	Query whether a secure random generator has experienced a catastrophic error	Data, API Call Parameters	Status Message	None
LmiSecureRandomGeneratorReseed	Reseed the module's approved DRBG	Data, API Call Parameters	Keys, Status Message	DRBG "V" Value – W DRBG "Key" Value – W DRBG Seed – X
LmiSecurityCalculateFingerprint	Calculate and return the fingerprint (HMAC SHA-1 value) of the Vidyo SDK security kernel in an application	CSK image, API Call Parameters	Status Message	HMAC Key – R
LmiSecurityInitialize	Initialize all security-related components of the Vidyo SDK	API Call Parameters	Status Message	All –RWX
LmiSecurityIsInitialized	Query whether the security-related components of the Vidyo SDK are currently initialized	API Call Parameters	Status Message	None
LmiSecurityUninitialize	Uninitialize all security-related components of the Vidyo SDK	API Call Parameters	None	All –W
LmiSha1CtxAssign	Assign a SHA-1 context as a copy of an existing one. All states previously associated with the target context is overwritten	Data, API Call Parameters	Data, Status Message	None

Service	Description	Input	Output	CSP and Type of Access
LmiSha1CtxConstruct	Construct and initialize a SHA-1 context	API Call Parameters	Data, Status Message	None
LmiSha1CtxConstructCopy	Construct a SHA-1 context as a copy of an existing one	Data, API Call Parameters	Data, Status Message	None
LmiSha1CtxDestruct	Destruct a SHA-1 context, completely erasing its internal state	Data, API Call Parameters	None	None
LmiSha1CtxFinal	Finalize a SHA-1 context and retrieve its digest data	Data, API Call Parameters	Data, Hash, Status Message	None
LmiSha1CtxUpdate	Update a SHA-1 context with message data to be hashed	Data, Message, API Call Parameters	Data, Status Message	None

2.5 Physical Security

The Cryptographic Security Kernel is a software module and does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on a host GPC hardware platform running the following operating environments:

- Full software implementations:
    - Linux Ubuntu 10.04 (x86) on Intel Xeon E50xx
    - Linux Ubuntu 10.04 (x64) on Intel Xeon E50xx
    - Mac OS X 10.6.8 (x86) on Intel Core Duo
    - Mac OS X 10.6.8 (x64) on Intel Core 2 Duo
    - Mac OS X 10.7.3 (x86) on Intel Core 2 Duo
    - Mac OS X 10.7.3 (x64) on Intel Core 2 Duo
    - Windows 7 (x86) on Intel Core Duo
    - Windows 7 (x64) on Intel Core 2 Duo
    - Windows XP (x86) on Intel Core Duo
- Implementations employing hardware support for AES and SHA-1:
    - Linux Ubuntu 10.04 (x86) on Intel Xeon E3
    - Linux Ubuntu 10.04 (x64) on Intel Xeon E3
    - Mac OS X 10.6.8 (x86) on Intel Core i5
    - Mac OS X 10.6.8 (x64) on Intel Core i5
    - Mac OS X 10.7.3 (x86) on Intel Core i5
    - Mac OS X 10.7.3 (x64) on Intel Core i5
    - Windows 7 (x86) on Intel Core i5
    - Windows 7 (x64) on Intel Core i5
    - Windows XP (x86) on Intel Core i5

Vidyo affirms that the module also executes in its FIPS-Approved manner on other operating systems that are binary-compatible to those on which the module was tested. All cryptographic keys and CSPs are under the control of the operating system, which protects the CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API.

2.7 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 4 below.

Table 4 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	Software Implementation	Hardware-Supported Implementation
AES in ECB[10], CTR[11] mode (128-/192-/256-bit keys)	2027	2028
SHA-1	1776	1777
HMAC[12] SHA-1	1229	1230
NIST[13] SP[14] 800-90 CTR_DRBG[15]	194	195

The module supports the critical security parameters (CSPs) listed below in Table 5.

Table 5 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key Type	Generation / Input	Output	Storage	Zeroization	Use
AES Key	AES 128-, 192-, 256-bit key	Generated internally	API Call	Plaintext in volatile memory	API call or power cycle	Encryption and decryption of data
HMAC Key	HMAC Key	Generated internally	API Call	Plaintext in volatile memory	API call or power cycle	Message authentication
DRBG "V" Value	Internal CTR DRBG state value	Generated Externally and Input in Plaintext	Never	Plaintext in volatile memory	API call or power cycle	Used for SP 800-90 CTR_DRBG
DRBG "Key" Value	Internal CTR DRBG key value	Generated Externally and Input in Plaintext	Never	Plaintext in volatile memory	API call or power cycle	Used for SP 800-90 CTR_DRBG
DRBG Seed	Random bit value	Generated Externally and Input in Plaintext	Never	Plaintext in volatile memory	API call or power cycle	Seed input to SP 800-90 CTR_DRBG

[10] ECB – Electronic Code Book
[11] CTR - Counter
[12] HMAC – (Keyed-) Hashed Message Authentication Code
[13] NIST – National Institute of Standards and Technology
[14] SP – Special Publication
[15] CTR_DRBG – CTR Deterministic Random Bit Generator

2.8 Self-Tests

The Vidyo Cryptographic Security Kernel performs a set of self-tests upon power-up and conditionally during operation as required in FIPS 140-2.

2.8.1 Power-Up Self-Tests

The module runs power-up self tests when the module has been loaded into the host GPC's memory for execution and when they are called on-demand via power-cycling the host system. If all power-up self-tests pass, the module will continue to function. If a self-test fails, the module will incur an error and will have to be restarted to in order to bring the module back to functionality.

The Cryptographic Security Kernel performs the following self-tests at power-up:

- Software integrity check using a Message Authentication Code (HMAC SHA-1)
- Known Answer Tests (KATs)
  - AES KAT
  - SHA-1 KAT
  - HMAC SHA-1 KAT
  - SP 800-90 CTR_DRBG KAT

A self-test failure causes the module to enter an error state. The module is capable of checking status and performing an integrity test in this state. Unloading the module effectively inhibits all data output and prevents the use of any of its cryptographic functionality until the error state is cleared by reloading the module.

2.8.2 Conditional Self-Tests

The Cryptographic Security Kernel performs a Continuous RNG Test whenever a random number is generated. This ensures that the DRBG will output random numbers without being repeated. Failure of this self-test causes the module to enter an error state and will be unloaded. Unloading the module effectively inhibits all data output and prevents the use of any of its cryptographic functionality until the error state is cleared by reloading the module.

2.8.3 Critical Functions Tests

The Cryptographic Security Kernel runs critical functions tests whenever the random bit generator is instantiated and whenever it is reseeded. This ensures the random bit generator algorithm cannot be predicted. These tests are run simultaneously with the random bit generator conditional self-test. Should any of these tests fail, the module will enter an error state and will be unloaded. Unloading the module effectively inhibits all data output and prevents the use of any of its cryptographic functionality until the error state is cleared by reloading the module.

The Vidyo Cryptographic Security Kernel is also capable of using the host systems' CPU to assist with AES and SHA-1 operations (if the processor is so enabled). To determine whether the CPU embedded in the host GPC is able to assist in the AES and SHA-1 operations, the module will perform critical self-tests that request flags from the CPU that report whether or not AES-NI[16] and SSSE3[17,18] support is available. If the CPU reports support for both instruction sets, the module will employ the arithmetic instruction set on

[16] AES-NI – Advanced Encryption Standard – New Instructions (an extension to the x86 instruction set architecture comprising instructions for accelerating various sub-steps of the AES algorithm)

[17] SSSE3 – Supplemental Streaming SIMD Extensions 3 (an extension of the x86 instruction set architecture comprising instructions for increasing the performance of SHA-1 software implementations)

[18] SIMD – Single Instruction, Multiple Data

the processor. If the CPU does not support either AES-NI or SSSE3, the module will run pure software implementations of both AES and SHA-1 (outlined in this security policy).

The Cryptographic Security Kernel performs the following critical functions tests:

- SP 800-90 DRBG Instantiate Test
- SP 800-90 DRBG Reseed Test
- AES-NI-Enabled Processor Test
- SSSE3-Enabled Processor Test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

The Vidyo Cryptographic Security Kernel meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The Vidyo Cryptographic Security Kernel module is installed as part of the installation of a Vidyo software application or software development kit. For the CSK, the CO should follow the installation procedures of the Vidyo software application to insure proper installation and operation of the Vidyo CSK.

The Vidyo CSK does not input, output, or persistently store CSPs within its logical boundary. However, the module may store CSPs within the physical boundary of the host system on which it runs. Operators are responsible for providing persistent storage of the cryptographic keys and CSPs, and to ensure that keys are transmitted outside the physical cryptographic boundary in the appropriate manner.

3.2 Crypto Officer Guidance

It is the Crypto Officer's responsibility to ensure that the host operating system executing the module is configured to a "single user mode" of operation. The Crypto Officer should follow the appropriate operating system's instructions on how to place it into "single user mode". Guidance can be found on each operating system's website.

3.2.1 Installation

The module will be provided as a binary to the Crypto Officer by Vidyo. The module is installed during the process of installing the host application or software development kit. With the delivered software, the Crypto Officer also receives detailed documentation on installing, uninstalling, configuring, managing and upgrading the host application.

3.2.2 Management

The module itself requires no set-up or management, as it only executes in a FIPS-Approved mode of operation. When the module is powered up, it performs the required power-on self-tests automatically. If the power-up self-tests are passed, the module is deemed to be operating in FIPS mode.

3.3 User Guidance

The User does not have any ability to install or configure the module. Operators in the User role are able to use the services available to the User role listed in Table 3. However, they should report to the Crypto Officer if any irregular activity is noticed.

4 Acronyms

This section defines the acronyms used in this document.

Table 6 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard – New Instructions
API	Application Programming Interface
AVLA	Advanced Video Layering Architecture
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSK	Cryptographic Security Kernel
CSP	Critical Security Parameter
CTR	Counter
CTR_DRBG	CTR Deterministic Random Bit Generator
DVD	Digital Video Disc
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
RAM	Random Access Memory
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SIMD	Single Instruction, Multiple Data
SP	Special Publication
SSSE3	Supplemental Streaming SIMD Extensions 3

Acronym	Definition
SVC	Scalable Video Coding
USB	Universal Serial Bus

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com