BAE SYSTEMS

STOP 8 Kernel Cryptographic Module FIPS 140-2 Security Policy

BAE Systems

December 19, 2019

Version:	2.07
Version Date:	December 19, 2019
Title:	STOP 8 Kernel Cryptographic Module FIPS 140-2 Security Policy
Prepared by:	BAE Systems 11487 Sunset Hills Road Reston, VA 20190

Table of Contents

Table of Figures

List of Tables

1. Introduction

The following describes the security policy for the BAE Systems STOP 8 Kernel Cryptographic Module (Version 1.2.1). The STOP 8 Kernel Cryptographic Module provides FIPS-validated cryptographic operations including encrypting/decryption, MAC, hashing and random number capabilities to the STOP 8 Operating System Kernel via the module API. The Tested Operating Environment was: “BAE System STOP 8 Operating System running on BAE XTS-600-W-T with an Intel Xeon E5-1650”

The STOP 8 Kernel Cryptographic Module is a statically linked library that is linked into the monolithic kernel (see Figure 2). The module provides the cryptographic functionality required by the kernel to perform data protection functionality of the STOP 8’s encrypted filesystem. It also provides the secure random number generation functionality that is provided to the operating system users (via the /dev/urandom device).

Since the module is a software library designed to run on a general-purpose computer system, the embodiment is a multi-chip standalone device. The module is defined by the physical boundary of the general-purpose computer system and is logically defined by the static library (libcrypto.a) that is compiled into the kernel. This structure is not distributed as an independent file and is contained entirely within the monolithic kernel of the operating system.

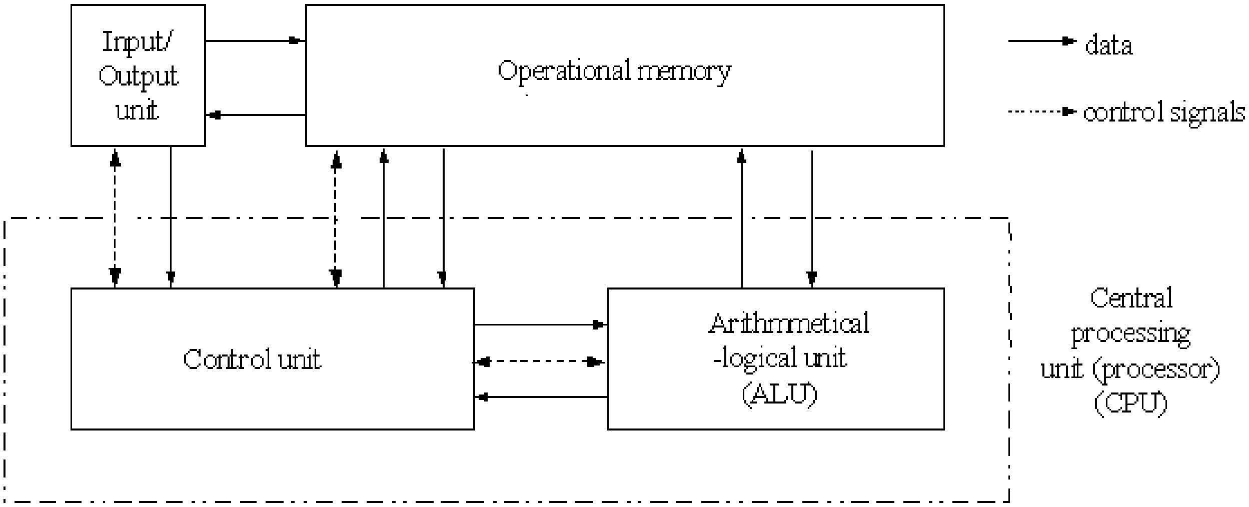

Figure 1: Typical general-purpose computer

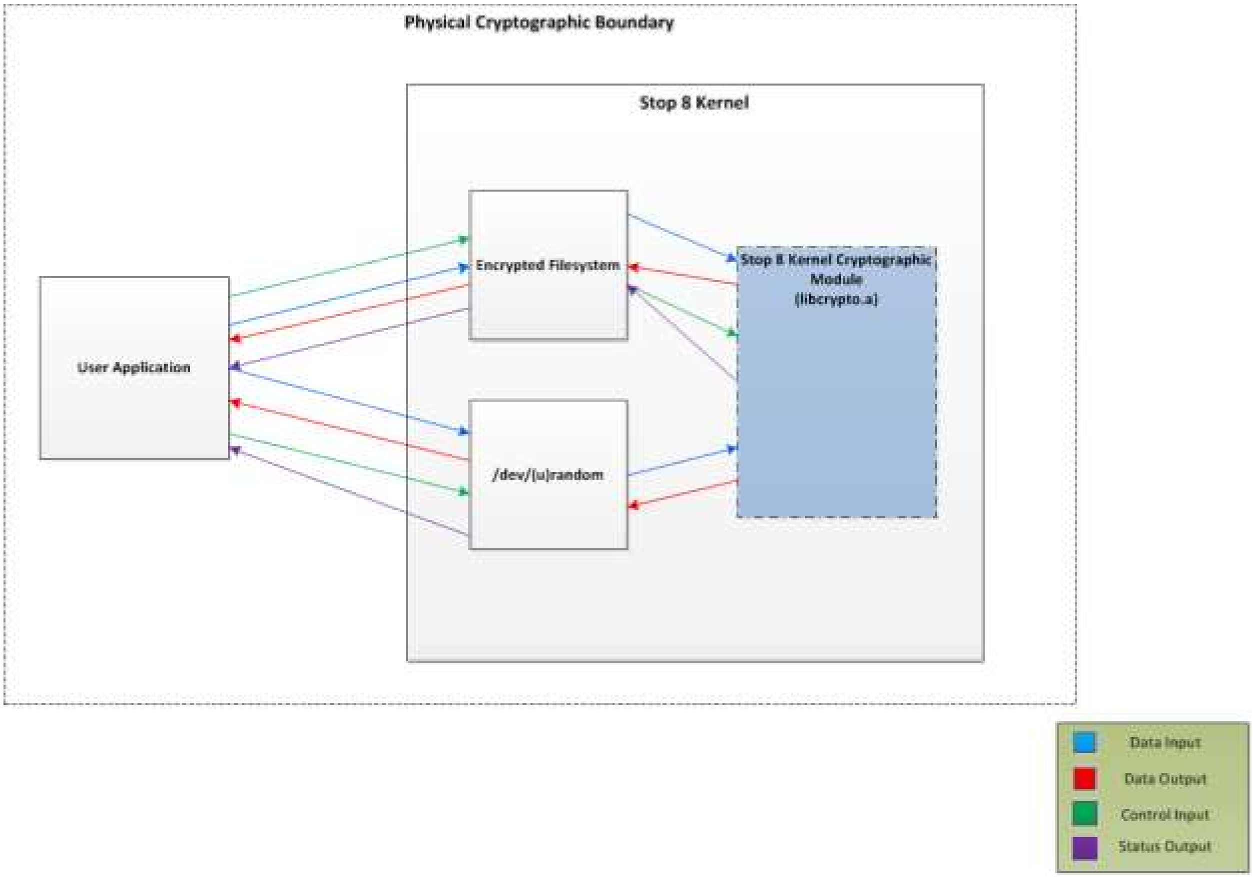

Figure 2: Cryptographic Module Diagram (boundary in blue)

1.1. Purpose

This document covers the secure operation of the STOP 8 Kernel Cryptographic Module including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

The module is being validated to FIPS 140-2 at an Overall Level 1. The table below details levels met by the module for each section of the FIPS 140-2 standard.

Table 1: Cryptographic Module Validation Levels

FIPS 140-2 Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services and Authentication	1

Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
Electromagnetic Interface/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

1.2. Module Ports and Interfaces

As a software-only module, the module does not have physical ports. For the purpose of the FIPS 140-2 validation, the physical ports are interpreted to be the physical ports of the hardware platform on which the module runs.

Table 2: Module Interface Mapping

FIPS 140-2 Interface	Logical Interface	Physical Interface
Data Input	Input parameters of API function calls	Keyboard
Data Output	Output parameters of API function calls	Display
Control Input	API function calls	Keyboard
Status Output	API Return Value and/or Output	Display, System Log
Power	Kernel Log File(s)	Physical Power Connector

2. Roles, Services, and Authentication

The STOP 8 Kernel Cryptographic Module provides two different roles and a set of services particular to each of the roles. The module does not support operator authentication, since it is a Level 1 validation, meaning that operators implicitly assume either the Crypto-Officer or User Role based on the service being performed.

2.1. Roles

The roles of the module include a Crypto-Officer and User Role. Each of these roles are implicitly assumed based on the service being performed by the operator.

2.1.1. User Role

The User Role has access to use the STOP 8 Kernel Cryptographic Module to perform the cryptographic operations available via the module API. While operating as a User, one can perform any of the following services:

- Encryption/Decryption
- HMAC
- Show Status
- Generate Random Value
- Zeroization

2.1.2. Crypto-officer Role

The Crypto-Officer Role has access to perform the administrative tasks of the STOP 8 Kernel Cryptographic Module. The Crypto-Officer must perform the installation of the STOP 8 Kernel Cryptographic Module, which is done by installing the monolithic STOP 8 kernel. Initialization is automatically performed by the monolithic STOP 8 kernel when the system is booted. The Crypto-Officer does not perform any of the cryptographic operations through the module API. While operating as the Crypto-officer, one can perform any of the following services:

- Install/Uninstall Module
- Perform self-tests

3. Secure Operation and Security Rules

In order to operate the STOP 8 Kernel Cryptographic Module securely, the operator should be aware of the security rules enforced by this security policy and should adhere to those rules in order to maintain operation in the FIPS approved mode.

3.1. Security Rules

The security rules enforced by this security policy define the behavior that must be followed by the operator of the STOP 8 Kernel Cryptographic Module in order to maintain the FIPS approved mode of operation.

3.1.1. FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The operator must observe these security rules to maintain the FIPS approved mode of operation.

1. The module must be used as part of the STOP 8 operating system running on an x86-compatible general-purpose computer.
2. The operator of the module shall only use the FIPS approved algorithms as noted in Section 3.2.
3. In accordance to NIST guidance, operators are responsible for insuring that a single Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit data blocks.

3.2. Cryptographic Algorithms

The STOP 8 Kernel Cryptographic Module provides many different cryptographic algorithms. Specifically, the module provides the following FIPS approved algorithms:

Table 3: FIPS Approved Algorithms

Algorithm Type	Details	Certificate
AES	128-, 192- and 256-bit, ECB and CBC	#5935
DRBG[1]	SP800-90 AES_CTR DRBG	#2488
HMAC	SHA-256	#3913
SHS	SHA-1, SHA-256, SHA-384, and SHA-512	#4690
Triple-DES	128 (Decrypt only)- and 192-bit, ECB	#2892

Not all of the algorithms/modes verified through the CAVP certificates are implemented by the module.

When the module is being used in a FIPS approved mode of operation, the operator should only make use of the FIPS approved algorithms identified above.

In addition, the module includes the following non-FIPS approved algorithms:

Table 4: Non-approved Algorithms

Algorithm Type	Details
DES	64-bit, ECB
NDRNG	Used to generate random values

[1] Used for supplying random numbers only, no key generation is performed by the module

3.2.1. Self-Tests

The STOP 8 Kernel Cryptographic Module implements the following self-tests, as required for FIPS 140-2:

- AES Known Answer Test
  - AES Encrypt Known Answer Test
  - AES Decrypt Known Answer Test
- DRBG Known Answer Test
- HMAC Known Answer Test
- SHS Known Answer Test (SHA-1, SHA-256, and SHA-512)
- Triple-DES Known Answer Test
  - Triple-DES Encrypt Known Answer Test
  - Triple-DES Decrypt Known Answer Test
- Software Integrity Test (HMAC-SHA-256)
- Conditional: SP 800-90A DRBG Health Tests
- Conditional: Continuous Random Number Generation Test (Approved and Non-approved RNG)

In the event of a self-test failure, the module enters the Error state, which triggers a kernel panic that inhibits further operations on the module. The Error condition can be cleared by an operator power-cycling the module.

4. Cryptographic Key Management

This section specifies the STOP 8 Kernel Cryptographic Module's key management, including the definition of cryptographic keys and critical security parameters.

4.1. Cryptographic Keys and CSPs

The STOP 8 Kernel Cryptographic Module supports the following cryptographic keys and critical security parameters:

Table 5: List of Keys/CSPs

Key/CSP	Description
Data Protection Keys	The AES and Triple-DES values used to perform encryption and decryption of data, which are provided through the module's API. These values are stored in plaintext in the RAM of the general-purpose computer system. It is zeroized by the caller of the module when no longer needed in memory.
Integrity Keys	The HMAC key (HMAC-SHA-256) values used to perform integrity calculation of data, which are provided through the module's API. These values are stored in plaintext in the RAM of the general-purpose computer system. It is zeroized when the requested operation is completed.
DRBG Key	The DRBG key value is one of the secret internal values of the SP800-90 DRBG and is generated as defined by SP800-90A. It is zeroized on system shutdown or reseed.
DRBG V	The DRBG V value is one of the secret internal values of the SP800-90 DRBG and is generated as defined by SP800-90A. It is zeroized on system shutdown or reseed.

4.2. Access Control Policy

The STOP 8 Kernel Cryptographic Module allows controlled access to the cryptographic keys and CSPs contained within it. The following table defines the access that an operator or application has to each key or CSP when performing a specified service for a given role. The permissions are categorized as a set of four permissions: read (r), write (w), execute (x), delete (z). If no permission is listed, then an operator outside the module has no access to the key or CSP.

Table 6: Key/CSP Access Control Policy

Key/CSP Access Policy	Keys and CSPs	Data Protection Keys	Integrity Keys	DRBG Key	DRBG V
Role/Service					
Crypto-Officer					
Install/uninstall Module					
Perform Self-Tests					
User					
Encryption/Decryption		wx			
HMAC			wx		
Show Status					
Generate Random Value				wx	wx
Zeroization		z	z	z	z

5. Appendices

5.1. Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
HMAC	Hash-based Message Authentication Code
RNG	Random Number Generator
SHA	Secure Hash Algorithm
STOP	Secure Trusted Operating Platform