Attivo Cryptographic Provider

Version 1.0

FIPS 140-2 Level 1
Non-Proprietary Security Policy

Version Number: 1.9
Date: September 01, 2017

Table of Contents

1. Module Overview

Attivo Cryptographic Provider is a component of Attivo Networks Inc.'s products such as the Attivo Central Manager 200, BOTsink 3200, and BOTsink 5100. These products constitute the Attivo ThreatMatrix Deception and Response Platform which detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving attackers into revealing themselves. The detections along with comprehensive attack analysis and actionable alerts empower accelerated incident response.

The cryptographic module is a software module that is executing in a modifiable operational environment by a general purpose computer.

This software module contains a single component:

- bc-fips.jar

FIPS 140-2 conformance testing was performed at Security Level 1. The following configuration was tested by the lab.

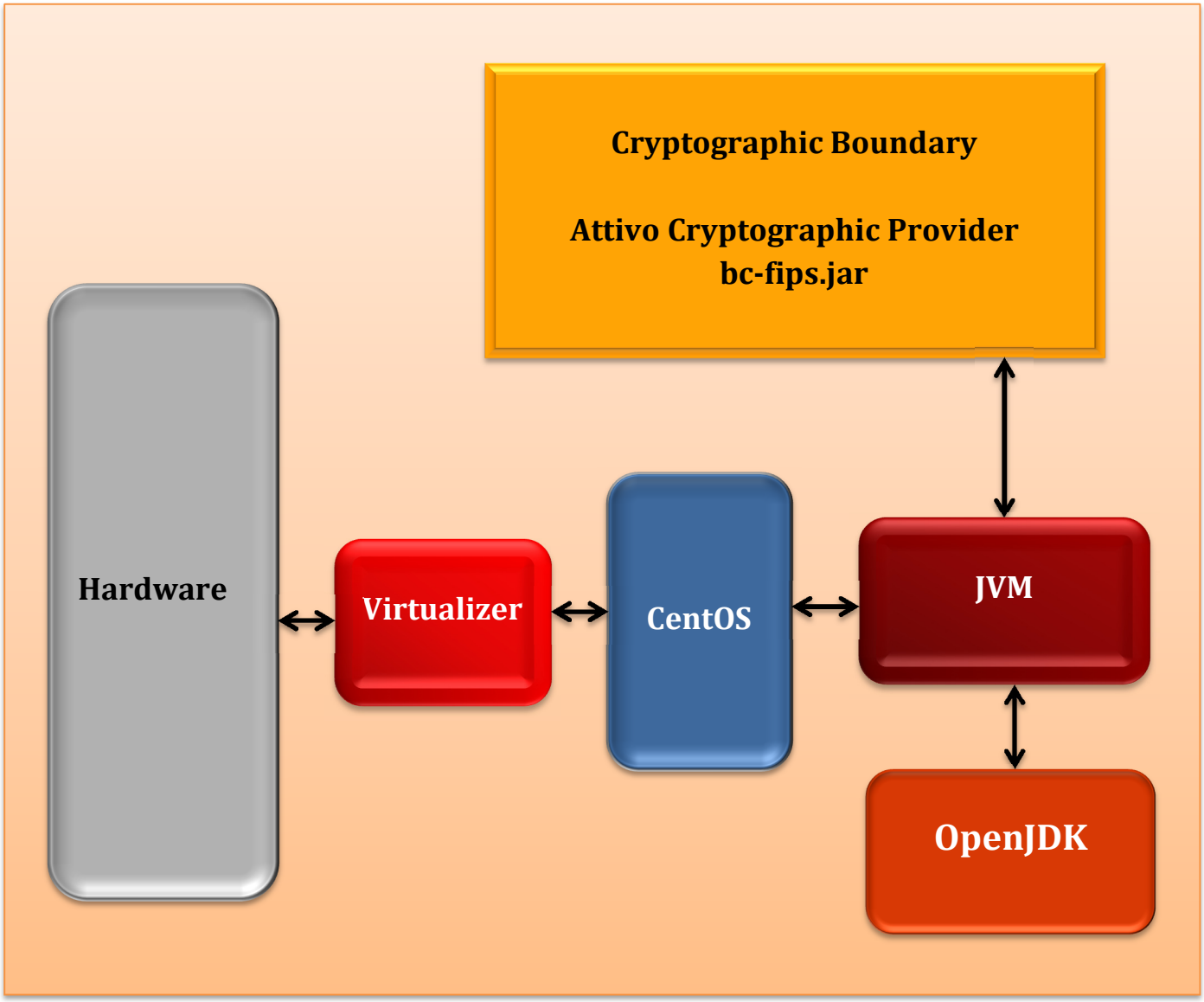
Table 1.1: Configuration tested by the lab

Software Component	Operating System	Processor(s)
● bc-fips.jar	Open JDK 1.8 on CentOS 6.5 Intel 64-bit on ESXi 5.5.0	Intel(R) Xeon(R) CPU E5-2620 v2 @2.10GHz

Table 1.2: Module Security Level Statement

FIPS Security Area	Security Level
Cryptographic Module Specification	1
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
EMI/EMC	1
Self-tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 1: Block Diagram for Attivo Cryptographic Provider



2. Modes of Operation

The module supports two modes of operation: Approved and Non-approved. CryptoServicesRegistrar.isInApprovedOnlyMode() method can be used to check the mode of operation.

The FIPS approved mode of operation is enabled by calling CryptoServicesRegistrar.setApprovedMode(true).

Non-approved algorithms are not available in the FIPS approved mode of operation.

2.1 Approved and Allowed Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.1: Approved Cryptographic Functions.

Algorithm	CAVP Certificate
AES (ECB, CBC, CBC-CS1, CBC-CS2, CBC-CS3, OFB, CFB8, CFB128, CTR, GCM, CCM and CMAC): 128/192/256 bits key	4049
DRBG SP 800-90A (CTR, Hash, HMAC)	1213
HMAC (SHA1, SHA224, SHA256, SHA384, SHA512, SHA-512/224, SHA-512/256)	2644
SHA (SHA1, SHA224, SHA256, SHA384, SHA512, SHA-512/224, SHA-512/256)	3339
SHA-3, SHAKE (SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)	9
KAS SP 800-56A-rev2 using FB, FC, EB, EC, ED, EE	90 and Vendor Affirmed
3 key Triple-DES (TECB, TCBC, TCFB, TOFB, CMAC, CTR) 2 key Triple-DES (decryption / unwrapping only)	2215
RSA (FIPS 186-4, FIPS 186-2, ANSI X9.31-1998 and PKCS #1 v2.1 (PSS and PKCS1.5)) Key Pair Gen, SigGen, SigVer, Component (as specified on the CAVP Certificates)	2084 879 (CVL)
DSA (FIPS 186-4) (PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver (as specified on the CAVP Certificate)	1095
ECDSA (FIPS 186-4) PKG, PKV, SigGen, SigVer, Component (as specified on the CAVP Certificates)	908 1190 (CVL)
KDF SP 800-135 (TLS v1.0/1.1 KDF, TLS 1.2 KDF, SSH KDF, X9.63 KDF, IKEv2 KDF, SRTP KDF)	878 (CVL)
KBKDF SP 800-108 (Modes: Counter Mode, Feedback Mode, Double-Pipeline Iteration Mode; Functions: CMAC-based KBKDF with AES, 2-key Triple-DES, 3-key Triple-DES or HMAC-based KBKDF with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)	99
Key Wrapping SP 800-38F (AES KW, KWP Key sizes: 128, 192, 256 bits; Triple-DES TKW Key size: 3-key)	4049 (AES) 2215 (TDES)

Algorithm	CAVP Certificate
Password-Based KDF (SP 800-132, PBKDF with Option 1a using HMAC-based KDF with SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) Note: keys derived from passwords, as described in SP 800-132, may only be used in storage applications. The user must only use 256-bit or stronger random passwords. The upper bound for the probability of having this parameter guessed at random is $1/2^{256}$.	Vendor Affirmed
Key Wrapping and Key Transport using RSA SP 800-56B	Vendor Affirmed

The following non-FIPS approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.2: Non-FIPS Approved But Allowed Cryptographic Functions.

Algorithm
RSA encrypt/decrypt using RSA with keys 2048 or 3072 bits key
DH using 2048-bit key
MD5 within TLS

2.2 All other algorithms

In the FIPS approved mode of operation the operator does not use the functions listed in the Table 2.3. These functions are available in the User role.

Table 2.3: Non-Approved Cryptographic Functions

Algorithm		
AES (non-compliant)	HMAC-MD5	RIPEMD-160
ARC4 (RC4)	HMAC-RIPEMD128	RIPEMD256
Blowfish	HMAC-RIPEMD160	RIPEMD320
Camellia	HMAC-RIPEMD256	RSA (non-compliant)
CAST5	HMAC-RIPEMD320	RSA KTS (non-compliant)
DES	HMAC-TIGER	SCrypt
Diffie-Hellman KAS (non-compliant)	HMAC-WHIRLPOOL	SEED

Algorithm		
DSA (non-compliant)	IDEA	Serpent
DSTU4145	KBKDF using SHA-512/224 or SHA-512/256 (non-compliant)	SipHash
ECDSA (non-compliant)	MD5	SHACAL-2
ElGamal	OpenSSL PBKDF (non-compliant)	TIGER
GOST28147	PKCS#12 PBKDF (non-compliant)	Triple-DES (non-compliant)
GOST3410-1994	PKCS#5 Scheme 1 PBKDF (non-compliant)	Twofish
GOST3410-2001	PRNG - X9.31	WHIRLPOOL
GOST3411	RC2	
HMAC-GOST3411	RIPEMD128	

3. Ports and interfaces

The physical ports of the module are the same as those of the computer system on which it is executing. The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: FIPS 140-2 Logical Interfaces

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and loads the module. The User uses the cryptographic services provided by the module. The module provides the following services.

Table 4: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Initialize	Crypto Officer	N/A
Self-test	Crypto Officer	N/A
Show status	User	N/A
Zeroize	User	All: Z
Installation	Crypto Officer	N/A
Random number generation	User	DRBG CSPs: R, W Keys: W
Asymmetric key generation	User	DSA keys: W ECDSA keys: W RSA keys: W
Symmetric encrypt/decrypt	User	AES key: R Triple-DES key: R
Symmetric digest	User	CMAC key: R
Message digest	User	N/A
Keyed Hash	User	HMAC key: R
Key transport	User	RSA keys: R
Key agreement	User	DH, SP 800-56A keys: R, W RSA keys: R Symmetric keys: W
Digital signature	User	RSA keys: R DSA keys: R ECDSA keys: R
SP 800-135 KDF	User	Secret input /output: R,W
SP 800-108 KDF	User	Secret input /output: R,W
SP 800-56A-rev2 Derivation Function	User	Secret input /output: R,W
PBKDF	User	Secret input /output: R,W HMAC key: R,W
Key wrapping / unwrapping	User	RSA key: R AES key: R Triple-DES key: R

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Utility functions	User	N/A

Non-Approved cryptographic services are implementations of Non-Approved algorithms. They are listed in the Section 2.2.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 5: Cryptographic Keys and CSPs

Key	Description/Usage	Origin	Zeroization
AES Key	Used during AES encryption, decryption, wrapping, generation and verification[1]	Generated using DRBG	Zeroized during power cycle or reboot
Triple-DES Key	Used during Triple-DES encryption, decryption, wrapping, generation and verification	Generated using DRBG	Zeroized during power cycle or reboot
HMAC Key	Used during calculation of HMAC	Generated using DRBG	Zeroized during power cycle or reboot
HMAC_DRBG CSPs: V(160/224/256/384/512 bits) and Key (160/224/256/384/512 bits), entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
AES CTR_DRBG CSPs: V (128 bits) and AES key (128/192/256 bits), entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
TDES CTR_DRBG CSPs: V (64 bits) and Triple-DES key (192 bits), entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot

[1] The AES-GCM IV is generated randomly using DRBG per IG A.5, and the IV length is at least 96 bits. Upon power cycle the calling application must ensure that any AES-GCM keys are refreshed.

Key	Description/Usage	Origin	Zeroization
Hash_DRBG CSPs: V (440/888 bits) and C (440/888 bits), entropy input (length depends on security strength)	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
RSA key pairs (≥2048 bits)	Used for Sign/Verify and Key wrapping	Generated using DRBG	Zeroized during power cycle or reboot
RSA verification keys (≥1024 bits)	Used for Verify	Provided by user	Zeroized during power cycle or reboot
DSA key pairs (2048/3072 bits)	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
DSA verification keys (1024/2048/3072 bits)	Used for Verify	Provided by user	Zeroized during power cycle or reboot
ECDSA FIPS 186-4 key pairs (All NIST defined B, K, and P curves >= 224 bits)	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
SP 800-56A-rev2 EC Agreement key pairs (All NIST defined B, K, and P curves >= 224 bits)	Used for key agreement	Generated by the module or provided by user	Zeroized during power cycle or reboot
SP 800-56A-rev2 and DH Key Pairs (>=2048 bits)	Used for key agreement	Generated by the module or provided by user	Zeroized during power cycle or reboot
KDF Secret Values	Used for key derivation	Generated by the module or provided by user	Zeroized during power cycle or reboot

The Keys and CSPs are stored in plaintext within the module. Keys and CSPs used in the FIPS Approved mode of operation shall not be used while in the non-FIPS mode of operation. Keys or CSPs shall not be established while in the non-FIPS mode of operation.

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

Table 6: Self-Tests

Algorithm	Test
Software integrity	KAT using HMAC-SHA256
HMAC	KAT using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
SHS	KAT using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512
AES	KAT (encryption/decryption/generation/verification)
Triple-DES	KAT (encryption/decryption/generation/verification)
RSA	KAT (Signature Generation, Signature Verification)
	Pairwise consistency test on generation of a key pair
Key Agreement Using RSA	KAT SP 800-56B KATs
Key Transport Using RSA	KAT SP 800-56B KATs
DSA	KAT (Signature Generation, Signature Verification)
	Pairwise consistency test on generation of a key pair
DRBG	KAT
	Continuous Random Number Generator test
	DRBG Health Checks
ECDSA	KAT (Signature Generation, Signature Verification)
	Pairwise consistency test on generation of a key pair
ECC KAS	KAT: Primitive “Z” Computation: FB
FFC KAS	KAT: Primitive “Z” Computation: FB
Extendable-Output functions (XOF)	KATs: Output Verification
NDRNG	Continuous Random Number Generator Test
DH	Pairwise consistency test on generation of a key pair
SP 800-56A	SP 800-56A Assurances

7. References

Table 7: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

Reference	Specification
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions