

The logo consists of the word "PENSANDO" in white, uppercase, sans-serif font, centered within a solid red rectangular background.

**Pensando Crypto Engine
by Pensando Systems, Inc.**

Version 1.0

FIPS 140-2 Level 1 Non-Proprietary Security Policy

Document Version Number: 1.3

Date: December 12, 2022

Table of Contents

1. Module Overview	3
2. Modes of Operation	5
3. Ports and interfaces	8
4. Physical Security	8
5. Roles and Services	9
6. Cryptographic Keys and CSPs	9
7. Self-tests	10
8. User Re-Compilation	10
9. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	10
10. References	11

1. Module Overview

The Pensando Systems Distributed Services Card (DSC) is a high-performance purpose-built PCIe card, typically deployed in servers and designed to offload and accelerate networking, security and storage functions. The DSC2-2Q200 supports several security services including the ability to accelerate AES-GCM and AES-XTS encryption/decryption in hardware offloads.

The cryptographic module is a multi-chip embedded software-hybrid cryptographic module within the DSC2-2Q200. The software version is 1.0, the hardware component of the module is the Pensando Cryptographic Accelerator, version 1.0.

The module provides cryptographic functions to accelerate cryptographic algorithms. The cryptographic functionality includes AES-GCM with 128 or 256-bit keys and AES-XTS with 128 or 256-bit keys.

The physical boundary is the physical perimeter of the DSC2-2Q200 itself.

The module provides AES-GCM and AES-XTS cryptographic acceleration to applications running on the DSC2-2Q200. The module's functions are accessed via an API defined by the module.

The module's operational environment is modifiable.

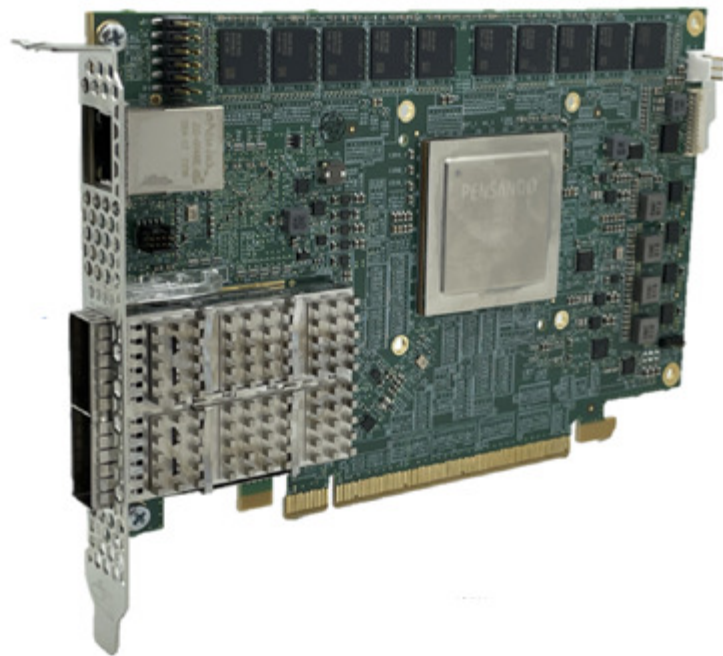


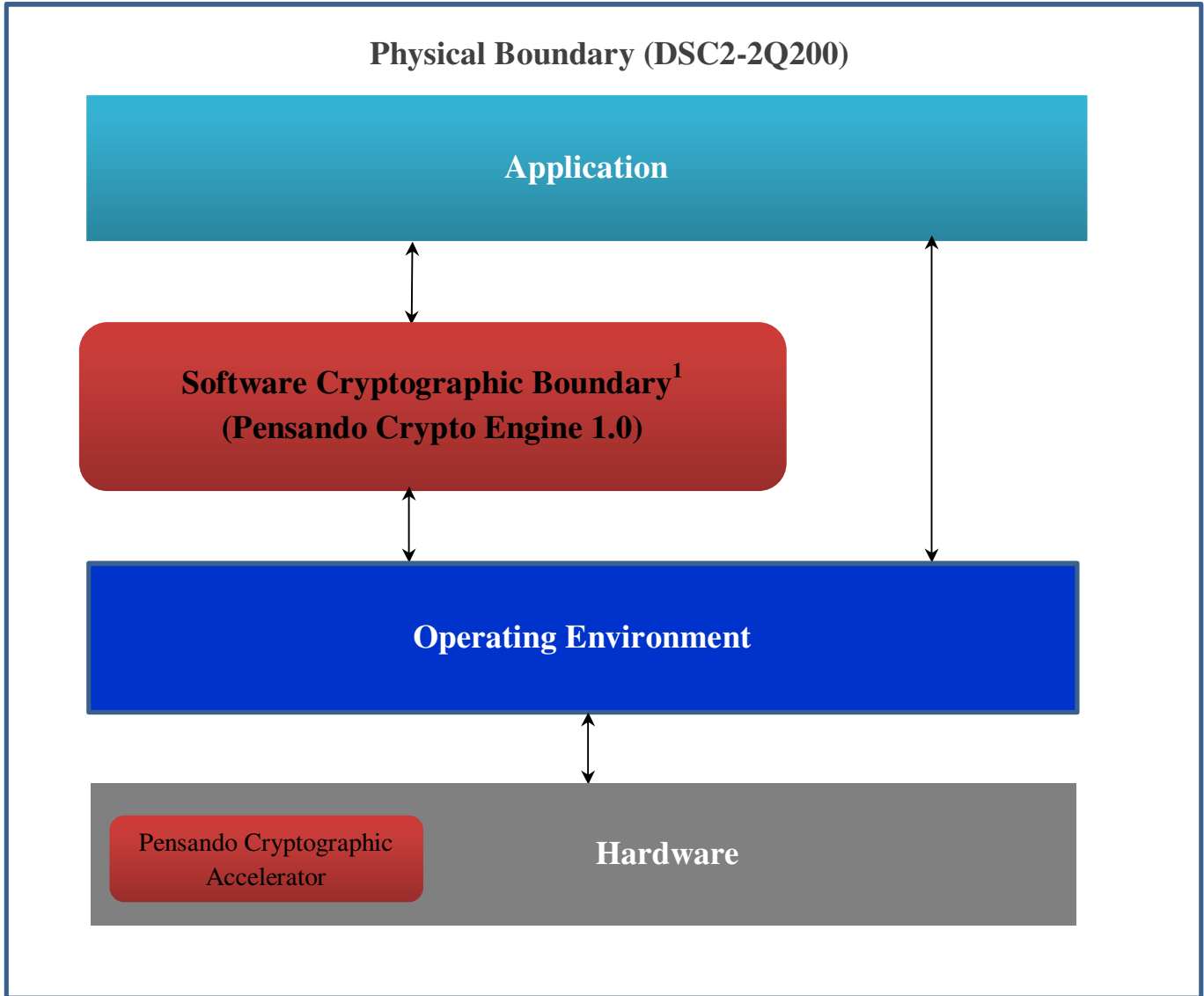
Table 1.1: Configuration tested by the lab


Module	Platform	Processor	Operating Systems
Pensando Crypto Engine	DSC2-2Q200	Cortex-A72	Linux 5.10.28

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	1
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 Pensando Crypto Engine



 Logical boundary

¹ libfips.so; libpenaccel_fips.so; libpenaccel_xts_keycheck.so; libpdsapi_athena_impl.so

2. Modes of Operation

The Pensando Crypto Engine supports the following two modes of operation to accommodate different operating requirements:

- 1) FIPS Approved mode of operation includes functions in Table 2.1.
- 2) FIPS Non-Approved mode of operation includes functions in Table 2.2.

The CSPs shall not be shared between the approved and non-approved modes.

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.

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A1030	Pensando Elba Inline Hardware Crypto Library	AES	FIPS 197, SP 800-38D	GCM ¹	128, 256	Encryption/ Decryption
A1128	Pensando Elba PenAccel Hardware Crypto Library	AES	FIPS 197, SP 800-38D, SP 800-38E	GCM ² , XTS	128, 256	Encryption/ Decryption

Note: There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

¹The module's AES-GCM implementation effectively complies with IG A.5 scenario 1: IPsec-v3 protocol IV generation. The module is compliant with RFC 4106. RFC 7296 compliant IKEv2 is used to establish the shared secret.

²The module's AES-GCM implementation effectively complies with:

- IG A.5 scenario 3: The module uses 32 bits of the IV field as a name and uses 64 bits as deterministic non-repetitive counter for a combined IV length of 96 bits
- IG A.5 scenario 1: IPsec-v3 protocol IV generation. The module is compliant with RFC 4106. RFC 7296 compliant IKEv2 is used to establish the shared secret.

In approved mode, the module shall not use GCM with an externally generated IV.

New AES-GCM keys are established if the module loses power.

Table 2.2: Non FIPS Approved Cryptographic Functions

Algorithm	Use
AES-ECB (non-compliant)	Encryption/Decryption
AES-CBC (non-compliant)	Encryption/Decryption
AES-CCM (non-compliant)	Encryption/Decryption and Message Authentication
HASH DRBG (non-compliant)	Random Number Generation
KAS ECC CDH-Component (non-compliant)	Shared Key Computation
ECDSA-SIGGEN (FIPS-186-4) (non-compliant)	Digital Signature
ECDSA-SIGVER (FIPS-186-4) (non-compliant)	Digital Signature
RSA-SIGGEN (FIPS-186-2)	Digital Signature Generation
RSA-SIGVER (FIPS-186-2) (non-compliant)	Digital Signature
RSA-SIGGEN (FIPS-186-4) (non-compliant)	Digital Signature
RSA-SIGVER (FIPS-186-4) (non-compliant)	Digital Signature
SHA-1 (non-compliant)	Hashing
SHA2-224 (non-compliant)	Hashing
SHA2-256 (non-compliant)	Hashing
SHA2-384 (non-compliant)	Hashing
SHA2-512 (non-compliant)	Hashing
SHA3-224 (non-compliant)	Hashing
SHA3-256 (non-compliant)	Hashing
SHA3-384 (non-compliant)	Hashing
SHA3-512 (non-compliant)	Hashing

Algorithm	Use
HMAC-SHA-1 (non-compliant)	Keyed Hash
HMAC-SHA-224 (non-compliant)	Keyed Hash
HMAC-SHA-256 (non-compliant)	Keyed Hash
HMAC-SHA-384 (non-compliant)	Keyed Hash
HMAC-SHA-512 (non-compliant)	Keyed Hash

3. Ports and interfaces

The physical ports of the module are the same as those of the DSC2-2Q200. The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: Logical Interfaces and Physical Ports

Logical Interface	Description	Physical Port
Data Input	Input parameters that are supplied to the API commands	<ul style="list-style-type: none"> • QSFP56 • PCIe • Serial • RJ45
Data Output	Output parameters that are returned by the API commands	<ul style="list-style-type: none"> • QSFP56 • PCIe • Serial • RJ45
Control Input	API commands	<ul style="list-style-type: none"> • PCIe • Serial • RJ45
Status Output	Return status provided by API commands	<ul style="list-style-type: none"> • PCIe • Serial • RJ45

4. Physical Security

The cryptographic module is a software-hybrid module that operates on a PCIe adapter that conforms to Level 1 requirements for physical security. The physical boundary of the module is the PCIe adapter. The cryptographic module consists of production-grade components that are embedded within a silicon ASIC mounted to the PCB board.

5. Roles and Services

The module supports the following roles:

User role: The user uses the cryptographic services provided by the module.

Crypto Officer role: The Crypto Officer installs and manages the module.

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
Installation	Crypto Officer	N/A
Initialize	Crypto Officer	N/A
Self-test	Crypto Officer	N/A
Show status	Crypto Officer User	N/A
Zeroization	Crypto Officer	All:Z
Reboot or shutdown	Crypto Officer	N/A
Inline AES-GCM encrypt/decrypt	User	Inline AES-GCM key: R
PenAccel AES-GCM encrypt/decrypt	User	PenAccel AES-GCM key: R
PenAccel AES-XTS encrypt/decrypt	User	PenAccel AES-XTS key: R

Non-Approved services are implementations of non FIPS Approved Cryptographic Functions. They are listed in the Table 2.2.

6. Cryptographic Keys and CSPs

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

Table 5: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
Inline AES-GCM 128/256 bit Key	Used during authenticated AES-GCM encryption / decryption	RAM in plaintext
PenAccel AES-GCM 128/256 bit Key	Used during authenticated AES-GCM encryption / decryption	RAM in plaintext
PenAccel XTS 128/256 bit Key	Used during AES-XTS encryption / decryption	RAM in plaintext

The Keys and CSPs are stored in plaintext in RAM within the module.

7. Self-tests

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

Table 6: Self-Tests

Algorithm	Test
Software integrity	AES-GCM
Inline AES-GCM	KAT(encryption/decryption)
PenAccel AES-GCM	KAT(encryption/decryption)
PenAccel AES-XTS	KAT(encryption/decryption)

8. User Re-Compilation

The Pensando Crypto Engine allows user re-compilation using the specified “make” command which provides the ability to build the binary software image with all compliant cryptographic functionality enabled.

Build Rule:

```
make PIPELINE=athena ASIC=elba ARCH=aarch64 PLATFORM=hw firmware
```

The source tarball integrity is protected against alteration using SHA-256. Another FIPS 140-2 validated implementation of SHA-256 must be used to verify the source tarball digest. The computed hash output must match the hash that is documented in the release note.

9. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The DSC2-2Q200 conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

10. 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

Reference	Specification
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[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