



October 1, 2025: Due to a lapse in federal funding, this website is not being updated. [Learn more.](#)

[PROJECTS](#)[CRYPTOGRAPHIC MODULE VALIDATION PROGRAM](#)[VALIDATED MODULES](#)[SEARCH](#)

Cryptographic Module Validation Program CMVP



PROJECT LINKS

[**Overview**](#)[**FAQs**](#)[**News & Updates**](#)

Publications

Certificate #4694

Details

Module Name

VMware's BoringCrypto Module

Standard

FIPS 140-2

Status

Active

Sunset Date

9/21/2026

Overall Level

1

Caveat

When operated in FIPS mode. No assurance of the minimum strength of generated keys.

Security Level Exceptions

- Physical Security: N/A
- Mitigation of Other Attacks: N/A

Module Type

Software

Embodiment

Multi-Chip Stand Alone

Description

VMware's BoringCrypto Module is a versatile software library that implements and provides FIPS 140-2 Approved cryptographic functionalities to various VMware products and services.

Tested Configuration(s)

- Amazon Linux 2 OS on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Amazon Linux 2 OS on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Amazon Linux 2023 OS on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Amazon Linux 2023 OS on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Photon OS 3.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Photon OS 3.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Photon OS 4.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Photon OS 4.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Photon OS 5.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Photon OS 5.0 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- RHEL 8.2 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- RHEL 8.2 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Ubuntu 20.04 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Ubuntu 20.04 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- Ubuntu 20.04 running on Dell Precision 5550 with Intel® Core I7 with PAA
- Ubuntu 20.04 running on Dell Precision 5550 with Intel® Core I7 without PAA
- Ubuntu 22.04 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- Ubuntu 22.04 on VMware ESXi 8.0 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA
- VMware ESXi 8.0U3 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 with PAA
- VMware ESXi 8.0U3 running on Dell PowerEdge R650 with Intel® Xeon Gold 6330 without PAA

Approved Algorithms

AES	Cert. # <u>A4970</u>
CVL	Cert. # A4970
DRBG	Cert. # A4970
ECDSA	Cert. # A4970

HMAC	Cert. # A4970
KAS	KAS-SSC Cert. # A4970, CVL Cert. #A4970
KAS-SSC	Cert. # A4970
KTS	AES Cert. # A4970; key establishment methodology provides between 128 and 256 bits of encryption strength
RSA	Cert. # A4970
SHS	Cert. # A4970
Triple-DES	Cert. # A4970

Allowed Algorithms

RSA (key wrapping; key establishment methodology provides between 112 and 256 bits of encryption strength)

Software Versions

6.0

Vendor

Broadcom Inc.

3401 Hillview Ave
Palo Alto, CA 94303
USA

Sunil Kumar Yadav

vcf.fips@broadcom.com

Phone: +91 (80671) 47256

Related Files

[Security Policy](#)

[Consolidated Certificate](#)

Validation History

Date	Type	Lab
4/24/2024	Initial	Acumen Security



HEADQUARTERS

100 Bureau Drive
Gaithersburg, MD 20899

Want updates about CSRC and our publications?

[Subscribe](#)

[Contact Us](#) | [Our Other Offices](#)

Send inquiries to csrc-inquiry@nist.gov

[Site Privacy](#) | [Accessibility](#) | [Privacy Program](#) | [Copyrights](#) | [Vulnerability Disclosure](#) | [No Fear Act Policy](#) | [FOIA](#) |

[Environmental Policy](#) | [Scientific Integrity](#) | [Information Quality Standards](#) | [Commerce.gov](#) | [Science.gov](#) | [USA.gov](#) |

[Vote.gov](#)