

September 26, 2022

To whom it may concern,

DEKRA's certified validation program tester has verified that the following 'Policy Compute Engine (PCE) version 22.2.30' of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

| Module Name | FIPS 140-2 Certificate |
|--|------------------------|
| Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module (Software Version: srhel8.20200305.1) | Cert. #3842 |
| Google, LLC BoringCrypto (Software Version: ae223d6138807a13006342edfeef32e813246b39) | Cert. #3678 |

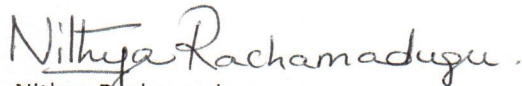
Red Hat Enterprise Linux 8.2

Illumio affirms that the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module (Software Version: srhel8.20200305.1) and the Google, LLC BoringCrypto (Software Version: ae223d6138807a13006342edfeef32e813246b39) used by the Illumio Policy Compute Engine (PCE) version 22.2.30 are built, initialized and operated in a manner that is FIPS 140-2 compliant, on the Red Hat Enterprise Linux 8.2 operating system using the associated FIPS 140-2 security policies (URLs below) as a reference:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3842.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3678.pdf>

Sincerely,



Nithya Rachamadugu
DEKRA Certification Inc.

August 17, 2022

To whom it may concern,

DEKRA's certified validation program tester has verified that the following 'Virtual Enforcement Node (VEN) version 22.2.30' of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

| Module Name | FIPS 140-2 Certificate |
|---|------------------------|
| Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module (Software Version: srhel8.20200305.1) | Cert. #3842 |
| Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module (Software Version: rhel8.20200327) | Cert. #3918 |

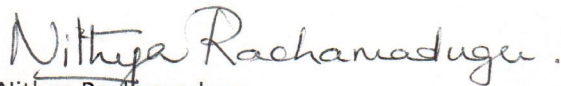
Red Hat Enterprise Linux 8.2

Illumio affirms that the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module (Software Version: srhel8.20200305.1) and the Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module (Software Version: rhel8.20200327) used by the Illumio Virtual Enforcement Node (VEN) version 22.2.30 are built, initialized and operated in a manner that is FIPS 140-2 compliant, on the Red Hat Enterprise Linux 8.2 operating system using the associated FIPS 140-2 security policies (URLs below) as a reference:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3842.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3918.pdf>

Sincerely,



Nithya Rachamadugu
DEKRA Certification Inc.

August 17, 2022

To whom it may concern,

DEKRA's certified validation program tester has verified that the following 'Virtual Enforcement Node (VEN) version 22.2.30' of Illumio, Inc. (Illumio) faithfully incorporates the cryptographic functions represented in the following cryptographic modules:

| Module Name | FIPS 140-2 Certificate |
|--|------------------------|
| Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2 (Software Versions: 6.3.9600 and 6.3.9600.17042) | Cert. #2356 |
| Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016 (Software Version: 10.0.14393 and 10.0.14393.1770) | Cert. #2936 |
| Kernel Mode Cryptographic Primitives Library (Software Version: 10.0.15063.674 [1], 10.0.15254 [2], 10.0.16299 [3], 10.0.17134 [4] and 10.0.17763 [5]) | Cert. #3196 |

Windows Server 2012 R2

Illumio affirms that the Microsoft Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2 (Software Versions: 6.3.9600 and 6.3.9600.17042) used by the Illumio Virtual Enforcement Node (VEN) version 22.2.30 is initialized and operated in a manner that is FIPS 140-2 compliant, on the Windows Server 2012 R2 operating system using the associated FIPS 140-2 security policy (URLs below) as a reference:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2356.pdf>

Windows Server 2016

Illumio affirms that the Kernel Mode Cryptographic Primitives Library (cng.sys) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016 (Software Version: 10.0.14393 and 10.0.14393.1770) used by the Illumio Virtual Enforcement Node (VEN) version 22.2.30 is initialized and operated in a manner that is FIPS 140-2 compliant, on the Windows Server 2016 and Windows 10 Enterprise operating systems using the associated FIPS 140-2

security policy (URLs below) as a reference:


<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2936.pdf>

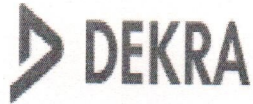
Windows Server 2019

Illumio affirms that the Kernel Mode Cryptographic Primitives Library (Software Version: 10.0.15063.674 [1], 10.0.15254 [2], 10.0.16299 [3], 10.0.17134 [4] and 10.0.17763 [5]) used by the Illumio Virtual Enforcement Node (VEN) version 22.2.30 is initialized and operated in a manner that is FIPS 140-2 compliant, on the Windows Server 2019 operating system using the associated FIPS 140-2 security policy (URLs below) as a reference:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3196.pdf>

Sincerely,


Nithya Rachamadugu
DEKRA Certification Inc.



On the safe side.

405 Glenn Dr #12
Sterling, VA 20164
(703) 657-2000

September 26, 2022

To whom it may concern,

DEKRA's certified validation program tester has verified that the following Illumio, Inc. (Illumio) products faithfully incorporate the use of the cryptographic functions provided by the FIPS 140-2 validated modules detailed below.

- Policy Compute Engine (PCE) version 22.2.30 on Red Hat Enterprise Linux 8.2
- Virtual Enforcement Node (VEN) version 22.2.30 on Red Hat Enterprise Linux 8.2
- Virtual Enforcement Node (VEN) version 22.2.30 on Windows Server 2012 R2, Windows Server 2016, Windows 10 Enterprise, and Windows Server 2019

The cryptographic operations performed apply to data in transit. The specific uses of the FIPS 140-2 validated modules with the Illumio products are specified as follows:

- Policy Compute Engine (PCE) version 22.2.30 on Red Hat Enterprise Linux 8.2: Illumio affirms that the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module and the Google, LLC BoringCrypto modules are built, initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

The associated security policies and CMVP caveat can be found here:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3842.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3678.pdf>

- Virtual Enforcement Node (VEN) version 22.2.30 on Red Hat Enterprise Linux 8.2: Illumio affirms that the Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module and the Red Hat Enterprise Linux 8 Kernel Crypto API Cryptographic Module modules are built, initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

The associated security policies and CMVP caveat can be found here:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3842.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3918.pdf>

- Virtual Enforcement Node (VEN) version 22.2.30 on Windows Server 2012 R2, Windows Server 2016, Windows 10 Enterprise, and Windows Server 2019: Illumio affirms that the Microsoft Kernel Mode Cryptographic Primitives Library (cng.sys) module is initialized and operated in a manner that is FIPS 140-2 compliant, as per the associated security policies and applicable CMVP caveat.

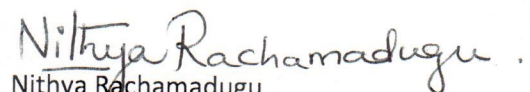
The associated security policies and CMVP caveat can be found here:

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2356.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2936.pdf>

<https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp3196.pdf>

Sincerely,


Nithya Rachamadugu
DEKRA Certification Inc.