



April 15, 2025

To Whom It May Concern:

A compliance review of Cisco Connected Mobile Experiences (CMX) with software version 11.1 was completed and found that the Product incorporates the following FIPS 140-2 and FIPS 140-3 validated cryptographic modules:

- Cisco FIPS Object Module version 7.2a (Certificate [#4036](#)) – FIPS 140-2
- Bouncy Castle FIPS Java API 2.0 (Certificate [#4743](#)) – FIPS 140-3

Cisco confirms that the cryptographic module listed above provides cryptographic services for the following as applicable:

- SSH, TLS, IPSec/IKEv2 – FOM version 7.2a
- Hyperlocation, NMSP, HAProxy – Bouncy Castle FIPS Java API 2.0

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All applicable cryptographic algorithms used for the services listed above are handled within the cryptographic module.
3. All applicable underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program ([CMVP](#)). The CMVP has not independently evaluated this compliance review.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at certteam@cisco.com.

Sincerely,

A handwritten signature in black ink that reads "Edward D. Paradise".

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security