December 8, 2015

To Whom It May Concern,

Acumen Security verified that the following software faithfully embeds a FIPS 140 validated cryptographic module,

- DX650, DX70, and DX80 firmware version 10.2

The software is known to operate on the following platforms:

- Cisco DX650,
- Cisco DX70,
- Cisco DX80.

As part of this review, the software was tested on the following platforms: Cisco DX70.

During the course of the review, Acumen Security confirmed that the following cryptographic module is incorporated into the product: **Cisco FIPS Object Module, version 4.1, FIPS 140-2 certificate # 2100**

Acumen Security confirmed that the following features leverage the embedded module to provide cryptographic services,

- Signaling Session Establishment, Encryption, and Authentication via TLS;
- Secure Storage;
- Authenticated CTL/ITL using Digital Signatures;
- File Authentication and Encryption;
- Media Streaming Session Establishment, Encryption, and Authentication via sRTP;
- Image Authentication.

For Signaling and Streaming Session Establishment, Encryption, and Authentication, either sRTP (Streaming) or TLS (Signaling) is provided by the embedded cryptographic module. In each instance, the following services are provided,

- All session establishment and key derivation,
- All bulk encryption,
- All packet authentication,
- All asymmetric authentication.

For Authenticated CTL/ITL and Image Authentication, the following services are provided,

- All hashing,
- All asymmetric authentication.

For Secure Storage, the following services are provided,

- All encryption,

For File Authentication and Encryption, the following services are provided,

- All encryption,
- All hashing,
- All asymmetric authentication.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

Ashit Vora
Laboratory Director