

Booz Allen Hamilton

CSTL

304 Sentinel Drive

Annapolis Junction

Maryland 20701

November 3, 2016

To whom it may concern,

1. The Booz Allen Hamilton CSTL has verified that the "AirWatch Core MDM Architecture version 9.x" faithfully uses the FIPS 140-2 Cryptographic Module BCryptPrimitives.dll (Software versions 6.3.9600 and 6.3.9600.17031, FIPS 140-2 Certificate #2357) for all of its cryptographic functionality, including for data at rest and data in transit. The security rules specified in the Security Policy for FIPS Certificate #2357 must be followed in order to put the BCryptPrimitives.dll into FIPS mode.

Booz Allen Hamilton:

- attests that the cryptography used by the AirWatch Core MDM Architecture version 9.x is FIPS compliant cryptography provided a user of the AirWatch Core MDM Architecture version 9.x follows the security rules found in the FIPS 140-2 Security Policy for CMVP certificate #2357.
 - attests that the AirWatch Core MDM Architecture version 9.x uses FIPS compliant cryptography on the validated platforms specified in section 1.3 of the FIPS 140-2 Security Policy for CMVP certificate #2357.
 - attests that AirWatch representatives will provide the correct installation instructions.
2. The Booz Allen Hamilton CSTL has verified that the "AirWatch iOS SDK version 5.x" faithfully uses the FIPS 140-2 Cryptographic Module Apple iOS CoreCrypto Module (Software version 6.0, FIPS 140-2 Certificate #2594) for all of its cryptographic functionality, including for data at rest and data in transit. The security rules specified in the Security Policy for FIPS Certificate #2594 must be followed in order to put the Apple iOS CoreCrypto Module into FIPS mode.

Booz Allen Hamilton:

- attests that the cryptography used by the AirWatch iOS SDK version 5.x is FIPS compliant cryptography provided a user of the AirWatch iOS SDK version 5.x follows the security rules found in the FIPS 140-2 Security Policy for CMVP certificate #2594.
- attests that the AirWatch iOS SDK version 5.x uses FIPS compliant cryptography on the validated platforms specified in section 2.1.3 of the FIPS 140-2 Security Policy for CMVP certificate #2594.
- attests that AirWatch representatives will provide the correct installation instructions.

- Attests that the AirWatch iOS SDK version 5.x makes calls to an OpenSSL cryptographic module but that all of these cryptographic function calls are “hooked” back to the Apple iOS CoreCrypto Module version 6.0
3. The Booz Allen Hamilton CSTL has verified that the “AirWatch Android SDK version 16.10” faithfully uses the FIPS 140-2 Cryptographic Module OpenSSL (Software version 2.0.13, FIPS 140-2 Certificate #2398) for all of its cryptographic functionality, including for data at rest and data in transit. The security rules specified in the Security Policy for FIPS Certificate #2398 must be followed in order to put the OpenSSL cryptographic module into FIPS mode.

Booz Allen Hamilton:

- attests that the cryptography used by the AirWatch Android SDK version 16.10 is FIPS compliant cryptography provided a user of the AirWatch Android SDK version 16.10 follows the security rules found in the FIPS 140-2 Security Policy for CMVP Certificate #2398.
 - attests that the AirWatch Android SDK version 16.10 uses FIPS compliant cryptography on the validated platforms specified in section 2 of the FIPS 140-2 Security Policy for CMVP certificate #2398.
 - attests that AirWatch correctly built, initialized and operated the OpenSSL cryptographic module by using the OpenSSL tar file version 2.0.13 with gcc compiler version 4.9.
 - attests that AirWatch representatives will provide the correct installation instructions.
4. The Booz Allen Hamilton CSTL has verified that the “AirWatch Windows 10 SDK version 1.0” faithfully uses the FIPS 140-2 Cryptographic Module BCryptPrimitives.dll (Software versions 10.0.10240 or 10.0.10586, FIPS 140-2 Certificate #2606) for all of its cryptographic functionality, including for data at rest and data in transit. The security rules specified in the Security Policy for FIPS Certificate #2606 must be followed in order to put the BCryptPrimitives.dll into FIPS mode.

Booz Allen Hamilton:

- attests that the cryptography used by the AirWatch Windows 10 SDK version 1.0 is FIPS compliant cryptography provided a user of the AirWatch Windows 10 SDK version 1.0 follows the security rules found in the FIPS 140-2 Security Policy for CMVP certificate #2606.
- attests that the AirWatch Windows 10 SDK version 1.0 uses FIPS compliant cryptography on the validated platforms specified in section 1.3 of the FIPS 140-2 Security Policy for CMVP certificate #2606.
- attests that AirWatch representatives will provide the correct installation instructions.



Eric Winterton

Laboratory Director

Booz Allen Hamilton CSTL