February 8, 2019

RE: FIPS 140-2 Compliance

Asavie Inc.
3455 Peachtree Road
5th Floor
Atlanta
Georgia
30326-02360

To Whom It May Concern:

This letter is in reference to the readiness of the **AccessMyLAN iOS App version 2.0.1** by Asavie Technologies for operation in a FIPS-compliant manner.

As issued by the National Institute of Standards and Technology (NIST), the Federal Information Processing Standard Publication 140-2 (FIPS 140-2) specifies the security requirements that must be satisfied by a cryptographic module used in a security system protecting sensitive but unclassified (SBU) information. Cryptographic modules can achieve FIPS-validation by undergoing a rigorous evaluation process overseen by the Cryptographic Module Validation Program (CMVP), co-sponsored by NIST and the Canadian Communications Security Establishment (CSE).

For a product to claim "FIPS-compliance", it should have some or all of its cryptographic security functions provided exclusively by cryptographic sources with active FIPS validations. The crypto source could be integrated into the product's application code or leveraged from the product's operational environment. Further, the product should employ the validated source(s) strictly according to the guidance specified in the cryptographic module's published Security Policy.

Based on a review of product architecture, features, operation, and testing results performed in Asavie Technologies' development facilities, Corsec Security, Inc. has made the following determinations:

- The AccessMyLAN iOS App software runs on iOS-based mobile devices with Apple's iOS versions 10 and 11.

- Apple's iOS 11 includes the Apple CoreCrypto Module v8.0 for ARM and Apple CoreCrypto Kernel Module v8.0 for ARM. Apple's iOS 10 includes the Apple CoreCrypto Module v7.0 for ARM and Apple CoreCrypto Kernel Module v7.0 for ARM.

- The Apple CoreCrypto and CoreCrypto Kernel Modules provide the cryptographic primitives necessary to support (1) the use of FIPS-Approved cipher suites associated with secure communications protocols and (2) the secure storage of sensitive items (including passwords, keys, and certificates) using FIPS-Approved cryptographic algorithms.

- Apple CoreCrypto Module v8.0 for ARM and Apple CoreCrypto Kernel Module v8.0 for ARM have been validated against FIPS 140-2 Level 1 requirements and, in 2018, were awarded cert #3148 and cert #3147 (respectively).

- Apple CoreCrypto Module v7.0 for ARM and Apple CoreCrypto Kernel Module v7.0 for ARM have been validated against FIPS 140-2 Level 1 requirements and, in 2018, were awarded cert #2827 and cert #2828 (respectively).

- While the AccessMyLAN iOS App acts as a consumer of the services provided by Apple's CoreCrypto and CoreCrypto Kernel Modules, there are no setup, installation, or configuration tasks that the iOS App software must perform. The iOS operating system will automatically initiate "all required tests such as the Power-On-Self-Tests (POST) for both the kernel and user space modules, integrity tests on the algorithms and module components, pairwise consistency tests, and finally the conditional self-tests on the random number generator".

In summary, when running on iOS 10 and iOS 11 and leveraging Apple's FIPS-validated CoreCrypto and CoreCrypto Kernel Modules (v7.0 or v8.0) in FIPS mode exclusively for cipher suite support and storage of secrets, the AccessMyLAN iOS App v2.0.1 use of FIPS-Approved cryptographic functions has been deemed **COMPLIANT** by Corsec's "FIPS Verified" evaluation for FIPS 140-2 compliance.

If there is any additional information I can provide on this matter, please do not hesitate to call me at (703) 267-6050.

Sincerely,

Digitally signed by John Morris
Date: 2019.02.11 10:32:25 -05'00'

John R. Morris
President, Corsec Security, Inc.

JM:hs