



Bulletin: FIPS 140-2 Validation of Ordr Products

April 2, 2020

Ordr products use the Ubuntu Linux Operating System as a base. Canonical Ltd., the commercial support arm of Ubuntu, has submitted all cryptographic modules used in Ubuntu to the Cryptographic Module Validation Program (CMVP) at the National Institute of Standards and Technology (NIST) for FIPS 140-2 Validation via the NIST accredited standards test lab, **atsec**, an information security corporation in Austin, TX.

All cryptographic modules have successfully received Certificates of Validation in compliance with requirements for the use of cryptography in government systems.

Ordr has engaged Ubuntu/Canonical to perform additional FIPS 140-2 validation testing for the cryptographic modules used by Ordr, on the hardware platforms used in their products. As a result, FIPS 140-2 Certificates of Validation, numbers [2888](#) for the Kernel Crypto module and [2962](#) for the OpenSSL module have been updated to include in special FIPS-enabled versions of the following Ordr hardware platforms – SCE-S2000, SCE-S1000, SCE-S500, SCE-A2000, and SCE-A1000. On the NIST website, they are listed as the Supermicro platforms running Ubuntu 16.04:

- Ubuntu 16.04 LTS 64-bit running on Supermicro SMX11SPL-F with PAA
- Ubuntu 16.04 LTS 64-bit running on Supermicro SMX11SPL-F without PAA (single-user mode)
- Ubuntu 16.04 LTS 64-bit running on Supermicro Supermicro A1SAi with PAA
- Ubuntu 16.04 LTS 64-bit running on Supermicro Supermicro A1SAi without PAA
- Ubuntu 16.04 LTS 64-bit running on Supermicro SYS-5018R-WR with PAA
- Ubuntu 16.04 LTS 64-bit running on Supermicro SYS-5018R-WR without PAA

All Ordr products installed on the above listed platforms use only FIPS 140-2 validated cryptography in compliance with US laws and meet all certification requirements for use of cryptography by the US government for sensitive but unclassified data.