

# Open Source Software Institute Press Release

Contact: John Weathersby  
Open Source Software Institute  
[jmw@oss-institute.org](mailto:jmw@oss-institute.org)  
662.236.1794

## OpenSSL Enters Evaluation for FIPS 140-2 Certification

**Oxford, MS – April 28, 2003** - The Open Source Software Institute ([www.oss-institute.org](http://www.oss-institute.org)) is leading an effort to secure National Institute of Standards and Technology's (NIST) FIPS 140-2 level 1 cryptographic certification for OpenSSL.

The Federal Information Processing Standards (FIPS) 140-2 validation specifies security requirements necessary for a cryptographic module to be utilized within government security systems protecting sensitive, but unclassified, information.

The OpenSSL software appears on the NIST Cryptographic Module Validation Program Pre-Validation List (<http://csrc.nist.gov/cryptval/preval.htm>) as "OpenSSL FIPS Cryptographic Module by Open Source Software Institute." The Pre-Validation list identifies certification efforts in progress. Final certification is expected in late 2003.

"OSSI is serving as the coordination body within the Open Source Community to help secure this important government certification for OpenSSL," said OSSI chairman, John Weathersby. "Our primary goal is to see that this software receives the FIPS 140-2 certification and then to ensure it remains accessible to all who wish to implement FIPS 140-2 approved cryptography."

Participating members in the certification effort include: Hewlett-Packard, DOMUS IT Security Laboratory, PreVal Specialists, Inc. and representatives from the OpenSSL Project.

Hewlett-Packard has provided funding to support the certification effort. In addition, Gary Gross, of HP, is serving as OSSI's program manager and technical lead for the FIPS 140-2 certification program.

OpenSSL, hosted and maintained by the OpenSSL Project ([www.openssl.org](http://www.openssl.org)), is a robust, commercial-grade, full-featured and open source toolkit implementing the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols as well as a full-strength general-purpose cryptographic library. The OpenSSL cryptographic library is widely used to provide the cryptography in products such as OpenSSH and Apache. Applications and products using the FIPS 140-2 certified OpenSSL cryptographic module for all cryptographic functions will themselves be FIPS 140-2 compliant and suitable for use in government programs.

Ben Laurie, a member of the OpenSSL core development team, is serving as the technical representative and OpenSSL community liaison during the pre-validation phase of the project. Peter Sargent, of Annapolis, MD-based PreVal Specialist, Inc., is providing documentation and pre-validation consulting services.

DOMUS IT Security Laboratory, a division of IBM Canada Limited, is serving as the NIST certified testing lab responsible for conducting algorithm and validation testing for the program.

### About OSSI

The Open Source Software Institute is a non-profit organization whose mission is to promote the development and implementation of open source software within the Federal government. Additional information on OSSI is available at [www.oss-institute.org](http://www.oss-institute.org).

# # #

<http://www.oss-institute.org>