



FOR IMMEDIATE RELEASE

Contact: John Weathersby
Executive Director, OSSI
Tel: 601.427.0152
Email: jmw@oss-institute.org

Program Review Briefing for the OpenSSL FIPS Validation Program

Hosted at Linux World Expo in Boston

Tuesday, April 4, Boston, MA – Representatives of the U.S. [Defense Medical Logistics Standard Support \(DMLSS\)](#) program, [DOMUS IT Security Labs](#), [Open Source Software Institute \(OSSI\)](#) and [OpenSSL.org Project](#) hosted a program briefing today at the Linux World Expo in Boston, MA to provide a program review for the recently announced FIPS 140-2 validation of OpenSSL.

OpenSSL is an open source library that provides cryptographic functionality to applications such as secure web servers. The CMVP, a joint effort between the U.S. National Institute of Standards and Technology (NIST) and the Canadian Communications Security Establishment (CSE), validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-2 and other cryptography-based standards. The FIPS 140-2 standard specifies the security requirements that are satisfied by a cryptographic module utilized within a security system protecting sensitive, but unclassified, information.

The official validation certificate (# **642**) called **OpenSSL FIPS Object Module by Open Source Software Institute** is posted at the NIST FIPS 140-1 and 140-2 Cryptographic Modules Validation List (<http://csrc.nist.gov/cryptval/140-1/1401val2006.htm>).

The validated OpenSSL module and source code will be available at the OpenSSL.org website and all security policy and user guide documents will be available for viewing and downloading from the OSSI website (www.oss-institute.org). According to the OpenSSL Project team members, the FIPS validated module will be included into the next OpenSSL release, which will be 0.9.7j. The validated version will be supported in subsequent releases by the OpenSSL.org Project.

The OpenSSL toolkit is licensed (<http://www.openssl.org/source/license.html>) under an Apache-style license, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

“This is an opportunity to discuss all aspects of this program in detail,” said OSSI executive director John Weathersby. “We are most fortunate that the final certification was issued right before Linux World. This gives us

a chance to answer questions directly and in person. It also provides the opportunity to lay out plans for the continued development of this validation effort.”

Specifics on the Validated OpenSSL Module

For the purposes of FIPS 140-2 validation the OpenSSL FIPS Object Module is defined as a binary library generated from a specific set and revision level of C language source files embedded within the OpenSSL source distribution. These source files are compiled to create a library that is used to provide a cryptographic API (Application Programming Interface) to external applications.

The OpenSSL FIPS library is a software cryptographic module that is generated from source code available for use on a wide variety of hardware and operating system platforms. The Module provides an API for invocation of FIPS approved cryptographic functions from calling applications. The portions of the full OpenSSL source distribution *external to and not included in the* Module are not considered FIPS 140 validated and non-FIPS approved algorithms other than DH are *disabled* while in FIPS mode. These non-validated algorithms include the Blowfish, CAST, IDEA, RC2, and RC4 algorithms.

The module was tested by the FIPS 140-2 Cryptographic Module Testing (CMT) laboratory for two specific test platforms, HP-UX 11i and SuSE Linux version 9.0. The OpenSSL FIPS Cryptographic Module, when generated from the identical unmodified source code, is "Vendor Affirmed" to be FIPS 140-2 compliant when running on other supported computer systems provided the conditions described in the *Security Policy* are met. On any platform the Module generated from the Module source code (the source files identified in Appendix B of the *Security Policy*) is *not* validated if that source code is modified in any way.

The OpenSSL FIPS library was designed and implemented to meet FIPS 140-2 requirements. As such, there are no special steps, other than building the binary library from the OpenSSL FIPS approved and HMAC-SHA-1 verified source code, and loading and initializing, required to ensure FIPS 140-2 compliant operation of the module. This process of generating the runtime application from source code is the same for all platforms and is documented in the *Security Policy*.

The OpenSSL FIPS library provides confidentiality, integrity, and message digest services. OpenSSL FIPS natively supports the following algorithms: DES, Triple DES, AES, RSA (for digital signatures), DH, DSA, SHA-1 and SHA-2. OpenSSL FIPS performs ANSI X9.31 compliant pseudo-random number generation.

About the Open Source Software Institute

The Open Source Software Institute (OSSI) is a U.S.-based non-profit organization whose mission is to promote the development and implementation of open source software solutions within U.S. Government agencies and academic entities. For additional information please visit the OSSI website at: www.oss-institute.org.

About Defense Medical Logistics Standard Support

The OpenSSL FIPS 140-2 validation effort was sponsored by the Defense Medical Logistics Standard Support program. The DMLSS Program, under the Assistant Secretary of Defense (Health Affairs) and the Deputy Under



Secretary of Defense (Logistics), is a partnership involving the wholesale medical logistics, medical information management, medical information technology, and user communities. The DMLSS mission is to improve responsiveness of medical logistics support. The DMLSS Program accomplishes this by implementing business process innovations that increase the effectiveness of medical logistics support and reduce cost. For additional information please visit the DMLSS website at: <http://www.tricare.osd.mil/dmlss/>.

About the OpenSSL.org Project

The [OpenSSL Project](http://www.openssl.org) is a collaborative effort to develop a robust, commercial-grade, full-featured, and open source toolkit implementing the Secure Socket Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan and develop the OpenSSL toolkit and its related documentation. For additional information please visit the OpenSSL.org Project website at: www.openssl.org.

About DOMUS IT Security Laboratory

DOMUS IT Security Laboratory in Ottawa, a unit of IBM Canada Ltd., is accredited by the US National Voluntary Laboratory Accreditation Program (NVLAP) to test cryptographic modules against the FIPS 140 standard. DOMUS IT Labs is also accredited by the Standards Council of Canada (SCC) to conduct Common Criteria Evaluation and Certification. For additional information please visit the DOMUS IT website at: <http://www.domusitsl.com/index.html> .

About PreVal Specialist, Inc.

PreVal Specialist, Inc., (PreVal) is a private security firm that works with organizations, companies and government entities to ease the burden of understanding and educating their personnel on International and US Cyber Security and Privacy Standards. For additional information contact Peter Sargent at: preval@att.net .

#