FIPS 140-2 Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Certificate No. **1080**

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the Cryptographic Module identified as:

BigFix Cryptographic Module *by* BigFix, Inc.
(When operated in FIPS mode)

in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive Information* (United States) or *Protected Information* (Canada) within computer and telecommunications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

This certificate includes details on the scope of conformance and validation authority signatures on the reverse.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module. The scope of conformance achieved by the cryptographic modules as tested in the product identified as:

BigFix Cryptographic Module *by* BigFix, Inc.
***(Software Version: 1.0;* Software)**

and tested by the Cryptographic Module Testing accredited laboratory: ***DOMUS IT Security Laboratory, NVLAP Lab Code 200017-0***
CRYPTIK Version 7.0
is as follows:

Cryptographic Module Specification:	Level 2	*Cryptographic Module Ports and Interfaces:*	Level 2
Roles, Services, and Authentication:	Level 3	*Finite State Model:*	Level 2
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 2
EMI/EMC:	Level 2	*Self-Tests:*	Level 2
Design Assurance:	Level 2	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 2	*tested in the following configuration(s):*	AIX 5.2 running on IBM P610; HP-UX 11.11 running on HP C3000; SUSE Linux Enterprise Server 9 running on IBM eServer 325; Mac OS X 10.3.6 running on iMac G4; Red Hat Enterprise Linux 4 Update 2 Advanced Server running on HP XW4100 Pentium 4; Red Hat Enterprise Linux 4 Update 2 Advanced Server 64-bit running on HP ProLiant DL145 G2; Solaris 9 SPARC running on Sun Blade 150; Solaris 10 SPARC running on Sun Blade 150; Solaris 10 x86 running on Dell Precision 650; Windows 2000 Pro with SP3 running on Dell Optiplex GX400; Windows 2003 Enterprise Edition with SP1 running on Dell Optiplex GX270; Windows XP Pro with SP2 running on Dell Optiplex GX270

The following FIPS approved Cryptographic Algorithms are used: **Triple-DES (Cert. #688); AES (Cert. #806); DSA (Cert. #298); SHS (Cert. #804); HMAC (Cert. #446); RSA (Cert. #388); RNG (Cert. #464)**

The cryptographic module also contains the following non-FIPS approved algorithms: **Diffie-Hellman; RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength)**

Overall Level Achieved: 2

Signed on behalf of the Government of the United States

Signature: William A Barker

Dated: January 9, 2009

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:

Dated: January 6, 2009

Director, Industry Program Group
Communications Security Establishment Canada