Cryptographic Module Validation Certificate

Certificate No.J0020

Cryptographic Module Name : Tahir Pak Crypto Library
Version : 2.1.1

Hardware Version : N/A
Firmware Version : N/A
Software Version : 2.1.1

Physical Embodiment : Multiple-chip standalone
Security Requirements : ISO/IEC 19790:2006 with ISO/IEC 19790:2006/Cor.1:2008
Testing Requirements : ISO/IEC 24759:2008

Vendor : Advanced Computing & Engineering Solutions (Pvt) LTD (ACES)
Address of Vendor : ACES, H.No 156, Street#5, F11/1, Islamabad, Pakistan
Special Affairs : When installed, initialized and configured as specified in the Security Policy Section 6.1

Notes : The cryptographic module identified in this certificate has been tested at an accredited Cryptographic Module Testing Laboratory in the Japan Cryptographic Module Validation Program, and the testing results have been validated in accordance with the Cryptographic Module Testing Requirements. This certificate applies only to the specific version of the Cryptographic Module in its tested configurations and operational environments. The Cryptographic Module Tests have been conducted in accordance with the provisions of the Japan Cryptographic Module Validation Program and the conclusions of the testing laboratory in the testing report are consistent with evidence adduced. This certificate is not an endorsement of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, and no warranty of the cryptographic module by the Information-technology Promotion Agency or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.
The misuse of this certificate, including the use of certificate for publications, such as advertisements and catalogs, in an incorrect or misleading manner may result in withdrawal of this certificate.

Signature : Original Signed Date : September 20, 2013
Name : Kazumasa Fujie
Title : Chairman
Information-technology Promotion Agency, Japan

Cryptographic Module Validation Report

The cryptographic module identified in this report has been validated in the following.

Cryptographic Module Name : Tahir Pak Crypto Library
Version : 2.1.1
Accredited Cryptographic Module Testing Laboratory : EPOCHE & ESPRI, S.L.U.
CRYPTIPA Version :1.2.2

Cryptographic Module Specification :	Level 2	*Cryptographic Module Ports and Interfaces :*	Level 2
Roles, Services, and Authentication :	Level 2	*Finite State Model :*	Level 2
Physical Security :	Level N/A	*Operational Environment :*	Level 2
Cryptographic Key Management :	Level 2	*Self-Tests :*	Level 2
Design Assurance :	Level 2	*Mitigation of Other Attacks :*	Level N/A

tested in the following configuration(s) : Red Hat Enterprise Linux 5.3 running on DELL PowerEdge T110II 11th

Overall Level Achieved : 2

The following Approved Cryptographic Algorithms are used :DSA (CAVP #733), AES (CAVP #2341), SHS (CAVP #2018), HMAC(CAVP #1450), DRBG(CAVP #291)

The cryptographic module also contains the following non approved algorithms : N/A

Test Results : Pass
The cryptographic module identified in this report has been tested on the basis of the testing requirements specified by the Japan Cryptographic Module Validation Program, and has achieved the scope of conformance to the specified security requirements from the test results.

Signature : Original Signed Date : September 20, 2013
Name : Kazumasa Fujie
Title : Chairman
Information-technology Promotion Agency, Japan