WOLF CREEK
NUCLEAR OPERATING CORPORATION

Stephen E. Hedges
Site Vice President

May 18, 2011
WO 11-0026

U. S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Information Security Branch
Washington, DC 20555

Reference: National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP)

Subject: Docket No. 50-482: Request for Approval of Secure Voice Communications CCORE Module by Cellcrypt Limited

Gentlemen:

Pursuant to 10CFR73.22(f)(3), Wolf Creek Nuclear Operating Corporation (WCNOC) hereby requests approval to utilize mobile telephone devices to transmit Safeguards information with the Cellcrypt Mobile application and the CCORE Cryptographic Module by Cellcrypt Limited. This module meets the requirements of Federal Information Processing Standard (FIPS) 140–2 approved by the Nuclear Regulatory Commission (NRC) per the latest validation list of the above reference. Enclosed is Validation Certificate No. 1310 for the subject module.

This letter contains no commitments. If you have any questions concerning this matter, please contact Mr. Scott Good at (620) 364-8831, Extension 4983, or Mr. David Erbe at (620) 364-8831, Extension 4973.

Sincerely,

Stephen E. Hedges

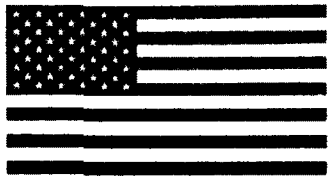
SEH/rlt

Enclosure

cc: E. E. Collins (NRC), w/e
J. R. Hall (NRC), w/e
G. B. Miller (NRC), w/e
Senior Resident Inspector (NRC), w/e

A001
NRR

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. **1310**

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:

CCORE Module *by* Cellcrypt Limited

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:

CCORE Module *by* Cellcrypt Limited
***(Software Version: 0.6.0-rc3;* Software)**

and tested by the Cryptographic Module Testing accredited laboratory: ***CEAL: a CygnaCom Solutions Laboratory, NVLAP Lab Code 200002-0***
CRYPTIK Version 7.0

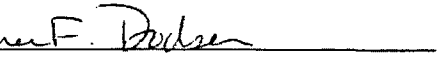
Cryptographic Module Specification:	Level 1	*Cryptographic Module Ports and Interfaces:*	Level 1
Roles, Services, and Authentication:	Level 1	*Finite State Model:*	Level 1
Physical Security: *(Multi-Chip Standalone)*	Level N/A	*Cryptographic Key Management:*	Level 1
EMI/EMC:	Level 1	*Self-Tests:*	Level 1
Design Assurance:	Level 1	*Mitigation of Other Attacks:*	Level N/A
Operational Environment:	Level 1	*tested in the following configuration(s):*	Ubuntu Server

The following FIPS approved Cryptographic Algorithms are used: **AES (Cert. #1089); RSA (Cert. #514); SHS (Cert. #1022); HMAC (Cert. #612); RNG (Cert. #611)**

The cryptographic module also contains the following non-FIPS approved algorithms: **RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength); RC4; MD5; EC Diffie-Hellman (non-compliant); ECDSA (non-compliant)**

Overall Level Achieved: 1

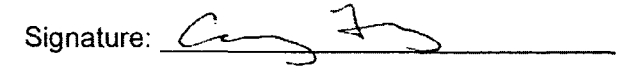
Signed on behalf of the Government of the United States

Signature: 

Dated: May 19, 2010

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: 

Dated: May 10, 2010

Director, Industry Program Group
Communications Security Establishment Canada