STP Nuclear Operating Company

South Texas Project Electric Generating Station P.O. Box 289 Wadsworth, Texas 77483

October 20, 2011
NOC-AE-11002738
10CFR73.22
STI: 32959429

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

South Texas Project
Units 1 & 2
Docket Nos. STN 50-498 & 50-499
Request For Approval Of Secure Voice Communications
CCORE Module By Cellcrypt Limited

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

Pursuant to 10CFR73.22(f)(3), STP Nuclear Operating Company 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. The module meets the requirements of Federal Information Processing Standard (FIPS) 140-2 approved by the Nuclear Regulatory Commission per the latest validation list of the above reference. Enclosed is Validation certificate No. 1310 for subject module.

There are no commitments in this letter.

If you have any questions on this matter, please contact Marilyn Kistler at (361) 972-8385 or me at (361) 972-4534.

G. O. Hildebrandt
Manager, Plant Protection

Enclosure: Validation certificate No. 1310

SD08
NRR

cc:
(paper copy)

Regional Administrator, Region IV
U. S. Nuclear Regulatory Commission
612 East Lamar Blvd, Suite 400
Arlington, Texas 76011-4125

Balwant K. Singal
Senior Project Manager
U.S. Nuclear Regulatory Commission
One White Flint North (MS 8 B1)
11555 Rockville Pike
Rockville, MD 20852

Senior Resident Inspector
U. S. Nuclear Regulatory Commission
P. O. Box 289, Mail Code: MN116
Wadsworth, TX 77483

C. M. Canady
City of Austin
Electric Utility Department
721 Barton Springs Road
Austin, TX 78704

U. S. Nuclear Regulatory Commission
Attention: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

(electronic copy)

A. H. Gutterman, Esquire
Morgan, Lewis & Bockius LLP

Balwant K. Singal
U. S. Nuclear Regulatory Commission

John Ragan
Chris O'Hara
Jim von Suskil
NRG South Texas LP

Kevin Pollo
Richard Pena
City Public Service

Peter Nemeth
Crain Caton & James, P.C.

C. Mele
City of Austin

Richard A. Ratliff
Texas Department of State Health
Services

Alice Rogers
Texas Department of State Health
Services

FIPS 140-2 Validation Certificate

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

FIPS VALIDATED 140-2 ™

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.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments.

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

is as follows:

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: Donna F. Dodson

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