March 12th, 2018

Independent Assurance Report

To the Management of Dubai Electronic Security Center (DESC):

Scope

We have been engaged, in a reasonable assurance engagement, to report on DESC management's assertion that in generating and protecting its "UAE Global Root CA G4 E2" on February 6th, 2018 at Dubai (UAE), with the following identifying information:

Root Name:	UAE Global Root CA G4 E2
Subject Key Identifier:	E0:64:8E:D9:5B:E0:4E:6A:7D:E4:C1:7C:88:C8:46:C7:E4:17:92:D8
Certificate Serial Number:	1F:D8:80:70:4B:C7:1C:38:00:00:00:00:5ª:79:68:6B
SHA256 Fingerprint:	51:A7:EC:B9:3A:CB:55:FF:0E:34:CD:0E:CF:D1:57:89:78:B3:7E:9E :DB:82:FD:06:F2:3F:6C:EC:00:5B:98:6D
SHA1 Fingerprint:	09:7A:E2:84:F5:8D:0A:BB:C3:9A:C6:71:F4:8C:E6:83:F8:6D:CB:2F

DESC has:

- followed the CA key generation and protection requirements in its:
  - Dubai PKI - Dubai Root CA - Certification Practice Statement_v1.0

- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
  - File "Root CA Key Ceremony Authorization Sheet 06022018.pdf"
  - File "Root CA Key Ceremony_06022018_Auditor Checklist.pdf"
  - File "Root CA Key Ceremony_06022018_Envelope Contents Verification.pdf"
  - File "Root CA Key Ceremony_06022018_Envelopes.pdf"
  - File "Root CA Key Ceremony_06022018_Personnel Roles.pdf"
  - File "Root CA Key Ceremony_06022018_Personnel.pdf"
  - File "Root CA Key Ceremony_06022018_Safes Keys Distribution.pdf"
  - File "Root CA Key Ceremony_06022018_Scope.pdf"
  - File "Root CA Key Ceremony _06022018 Luna G5 Domain owner PIN.pdf"
  - File "Root CA Key Ceremony _06022018 Luna G5 Partition MofN custodian PIN.pdf"
  - File "Root CA Key Ceremony _06022018 Luna G5 Partition Owner Password.pdf"

- o File "Root CA Key Ceremony _06022018 Luna G5 Security Officer PIN.pdf"
  - o File "Root CA Key Ceremony _06022018 Root CA First Officer Password.pdf"
  - o File "Root CA Key Ceremony _06022018 Root CA Master1 Password.pdf"
  - o File "Root CA Key Ceremony _06022018 Root CA Master2 Password.pdf"
  - o File "Root CA Key Ceremony _06022018 Root CA Master3 Password.pdf"
  - o File "Root CA Key Ceremony _06022018 Root CA Windows Administrator Password.pdf"
  - o File "Root CA Key Ceremony_06022018_Ceremony_Preparation.pdf"
  - o File "Root CA Key Ceremony_06022018_Laptops Preparation.pdf"
  - o File "Root CA Key Ceremony_06022018_Exception Handling.pdf"
  - o File "Root CA Key Ceremony_06022018_Exceptions.pdf"
  - o File "Root CA Key Ceremony_06022018_Root CA HSM Backup.pdf"
  - o File "Root CA Key Ceremony_06022018_Root CA.pdf"
  - o File "Root CA Key Ceremony_06022018_MofN custodian 1 key ceremony termination handover sheet.pdf"
  - o File "Root CA Key Ceremony_06022018_MofN custodian 2 key ceremony termination handover sheet.pdf"
  - o File "Root CA Key Ceremony_06022018_MofN custodian 3 key ceremony termination handover sheet.pdf"
  - o File "Root CA Key generation ceremony log.pdf"
  - o File "Transport DR equipment to DR Site.pdf"

- maintained effective controls to provide reasonable assurance that the DESC Root CAs were generated and protected in conformity with the procedures described in its CPS and its Root Key Generation Script(s)

- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)

- generated the CA keys in a physically secured environment as described in its CPS

- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge

- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CPS in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Certification authority's responsibilities

DESC's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

Auren applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of DESC's documented plan of procedures to be performed for the generation of the certification authority key pairs for the DESC Root CA;
(2) reviewing the detailed CA key generation script(s) for conformance with industry standard practices;
(3) testing and evaluating, during the CA key generation process, the effectiveness of controls over the integrity, confidentiality, and availability of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords), used in the establishment of the service;
(4) physical observation of all procedures performed during the root key generation process to ensure that the procedures actually performed on were in accordance with the Root Key Generation Script(s) for the DESC Root CAs; and
(5) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, in March 12th, 2018, DESC management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

This report does not include any representation as to the quality of DESC's services beyond those covered by CA Key Generation Criterion 4.1 of the

WebTrust Principles and Criteria for Certification Authorities v2.1, nor the suitability of any of DESC's services for any customer's intended purpose.

F. Mondragon, Auditor

auren

Valencia, SPAIN
March 12th, 2018

DESC MANAGEMENT'S ASSERTION

Dubai Electronic Security Center ("DESC") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy consistent of self-signed Root CA known as "UAE Global Root CA G4 E2". This CA will serve as Root CA for client certificate services. In order to allow the CA to be installed in a final production configuration, a Root Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA private signing key. This helps assure the non-refutability of the integrity of the DESC Root CA's key pair, and in particular, the private signing keys. DESC management has securely generated key pairs, consisting of a public and private key, in support of its CA operations.

The key pair was generated in accordance with procedures described in DESC's Certification Practice Statement (CPS), and its Root Key Generation Script(s), which are in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

DESC management established and maintained effective controls over the generation of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the root key generation process.

DESC management is responsible for establishing and maintaining procedures over its CA root key generations, and over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the DESC Root CA, and for the CA environment controls relevant to the generation and protection of its CA keys.

DESC management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generation and protecting its CA keys for the DESC Root CA's on February 6th, 2018 at Dubai (UAE), with the following identifying information:

Root Name:	UAE Global Root CA G4 E2
Subject Key Identifier:	E0:64:8E:D9:5B:E0:4E:6A:7D:E4:C1:7C:88:C8:46:C7:E4:17:92:D8
Certificate Serial Number:	1F:D8:80:70:4B:C7:1C:38:00:00:00:00:5ª:79:68:6B
SHA256 Fingerprint:	51:A7:EC:B9:3A:CB:55:FF:0E:34:CD:0E:CF:D1:57:89:78:B3:7E:9E :DB:82:FD:06:F2:3F:6C:EC:00:5B:98:6D
SHA1 Fingerprint:	09:7A:E2:84:F5:8D:0A:BB:C3:9A:C6:71:F4:8C:E6:83:F8:6D:CB:2F

DESC has:

- followed the CA key generation and protection requirements in its:
    - Dubai PKI - Dubai Root CA - Certification Practice Statement_v1.0
- included appropriate, detailed procedures and controls in its Root Key Generation Script(s):
    - File "Root CA Key Ceremony Authorization Sheet _06022018.pdf"
    - File "Root CA Key Ceremony_06022018_Auditor Checklist.pdf"
    - File "Root CA Key Ceremony_06022018_Envelope Contents Verification.pdf"
    - File "Root CA Key Ceremony_06022018_Envelopes.pdf"
    - File "Root CA Key Ceremony_06022018_Personnel Roles.pdf"

- o File "Root CA Key Ceremony_06022018_Personnel.pdf"
- o File "Root CA Key Ceremony_06022018_Safes Keys Distribution.pdf"
- o File "Root CA Key Ceremony_06022018_Scope.pdf"
- o File "Root CA Key Ceremony _06022018 Luna G5 Domain owner PIN.pdf"
- o File "Root CA Key Ceremony 06022018 Luna G5 Partition MofN custodian PIN.pdf"
- o File "Root CA Key Ceremony _06022018 Luna G5 Partition Owner Password.pdf"
- o File "Root CA Key Ceremony _06022018 Luna G5 Security Officer PIN.pdf"
- o File "Root CA Key Ceremony _06022018 Root CA First Officer Password.pdf"
- o File "Root CA Key Ceremony _06022018 Root CA Master1 Password.pdf"
- o File "Root CA Key Ceremony _06022018 Root CA Master2 Password.pdf"
- o File "Root CA Key Ceremony _06022018 Root CA Master3 Password.pdf"
- o File "Root CA Key Ceremony _06022018 Root CA Windows Administrator Password.pdf"
- o File "Root CA Key Ceremony_06022018_Ceremony_Preparation.pdf"
- o File "Root CA Key Ceremony_06022018_Laptops Preparation.pdf"
- o File "Root CA Key Ceremony_06022018_Exception Handling.pdf"
- o File "Root CA Key Ceremony_06022018_Exceptions.pdf"
- o File "Root CA Key Ceremony_06022018_Root CA HSM Backup.pdf"
- o File "Root CA Key Ceremony_06022018_Root CA.pdf"
- o File "Root CA Key Ceremony_06022018_MofN custodian 1 key ceremony termination handover sheet.pdf"
- o File "Root CA Key Ceremony_06022018_MofN custodian 2 key ceremony termination handover sheet.pdf"
- o File "Root CA Key Ceremony_06022018_MofN custodian 3 key ceremony termination handover sheet.pdf"
- o File "Root CA Key generation ceremony log.pdf"
- o File "Transport DR equipment to DR Site.pdf"

- maintained effective controls to provide reasonable assurance that the DESC Root CAs were generated and protected in conformity with the procedures described in its CPS and its Root Key Generation Script(s)
- performed, during the root key generation process, all procedures required by the Root Key Generation Script(s)
- generated the CA keys in a physically secured environment as described in its CPS
- generated the CA keys using personnel in trusted roles under multiple person control and split knowledge
- generated the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in its CP/CPS in accordance with CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.1.

Dr. Marwan Al Zarouni

Security Director

March 12th, 2018