Deloitte & Touche Advisory Saudi Limited
Prince Turki Bin Abdullah Al-Saud Street, Sulaimania Area, PO Box 213, Riyadh 11411, Kingdom of Saudi Arabia
Tel: +966 (11) 2828580
Fax: +966 (11) 4761350
www.deloitte.com

INDEPENDENT ASSURANCE REPORT

To the management of Baud Telecom Company ("BTC"):

Scope

We have been engaged, in a reasonable assurance engagement, to report on BTC management's assertion in generating and protecting the asymmetric key pair for its BTC Licensed Certificate Authority (CA) and EMDHA eSign CA on 16 December 2019 in Riyadh, Kingdom of Saudi Arabia, with the following identified information (full identified information enumerated in Attachment A):

CA Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint
BTC Licensed CA	b4 37 78 f2 5e 40 16 2f 17 e3 12 32 a4 03 c6 aa f8 43 0d 34	00db0e7b442047c2650 00000005c5228e2	B0:D8:31:88:C1:5A:95:BE:4 B:82:5E:A4:17:B1:2C:ED:62: 39:F8:BD:53:21:90:47:CE:89 :08:12:55:F3:01:CC
EMDHA eSign CA	04 93 7b 60 34 a9 b4 b8 28 28 f0 ff 43 aa 56 d1 94 ed a4 cc	32c8f771effdf11fcde7d5 0cefe7eb34	1C:F1:83:8F:F6:28:48:46:6F :2F:BF:15:98:25:8B:45:1D:3 9:4F:C6:F4:A2:0D:BF:70:29: C1:BF:43:A7:1C:BA

BTC has:

- Followed the CA keys generation and protection requirements in its:
  - BTC Licensed CA Certificate Policy/Certificate Practice Statement (CP/CPS), version 1.0, dated 12 December 2019;
  - EMDHA eSign CA Certificate Policy/Certificate Practice Statement (CP/CPS), version 1.0, dated 12 December 2019;
- Included appropriate, detailed procedures and controls in its key generation script:
  - BTC Licensed CA and EMDHA eSign CA, dated 12 December 2019;
- Maintained effective controls to provide reasonable assurance that the CA was generated and protected in conformity with the procedures described in its CP/CPS and its key generation script;
- Performed, during the key generation process, all procedures required by the key generation script;
- Generated the CA keys in a physically secured environment as described in its CP/CPS "5. Facility Management and Operational Controls";
- Generated the CA keys using personnel in trusted roles under multiple person control and split knowledge as described in its CP/CPS "5.2.2. Number of Persons Required per Task" and Key Generation Ceremony script; and
- Generated the CA keys within hardware cryptographic module (SafeNet Luna S750, firmware version 7.3.3) meeting the applicable technical and business requirements as disclosed in its CP/CPS "6.1.1. Key Pair Generation".

Certification authority's responsibilities

BTC's management is responsible for its assertion, including the fairness of its presentation, and for generating and protecting its CA keys in accordance with BTC's defined CP/CPS.

Our independence and quality control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm 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) Testing and evaluating, during the CA keys 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;
(2) Physical observation of all procedures performed during the CA keys generation process to ensure that the procedures actually performed on 16 December 2019 were in accordance with the key generation script for BTC Licensed CA and EMDHA eSign CA; and
(3) 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.

Inherent limitations

Because of the nature and inherent limitations of controls, BTC's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, on 16 December 2019, BTC 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 v2.2.

This report does not include any representation as to the quality of BTC CA's services beyond those covered by CA Key Generation Criterion 4.1 of the WebTrust Principles and Criteria for Certification Authorities v2.2, nor the suitability of any of BTC CA's services for any customer's intended purpose.

Deloitte & Touche Advisory Saudi Limited
20 January 2020

Attachment A

BTC Licensed CA Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            db:0e:7b:44:20:47:c2:65:00:00:00:00:5c:52:28:e2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = SA, O = National Center for Digital Certification, OU = Saudi National Root CA
        Validity
            Not Before: Dec 16 10:44:03 2019 GMT
            Not After : Nov 29 07:25:20 2029 GMT
        Subject: C = SA, O = Baud Telecom Company, CN = BTC Licensed CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:

                    00:a9:61:04:d7:02:29:9c:93:ec:36:f2:b6:87:30:b7:04:c0:b6:f4:dc:53:86:19:c9:a2:06:b1:5d:75:89:a4:a4:d3:ec:37:
                    10:c0:d9:74:b6:e1:b1:bd:6b:39:03:08:11:00:98:dd:8c:b1:f4:97:41:6c:3d:0f:d8:3e:56:f6:e0:97:e6:3f:e6:8e:06:78:7
                    6:04:5e:95:0d:3d:89:ac:1e:02:6d:7f:33:67:96:22:aa:9e:af:1e:06:fb:fc:a7:86:44:f5:00:c0:fa:96:f9:1e:d6:8a:53:e1:7
                    c:78:08:e9:2b:be:d5:a2:9f:2a:a2:88:b0:65:d0:dc:3e:bb:d9:e2:5f:24:0a:7c:ae:6f:2a:cf:ab:1d:8f:d8:ff:4c:3d:8e:d8:7f
                    :6f:9d:33:c0:f9:6d:c0:3d:a7:bb:03:58:43:ae:ee:fc:ed:20:45:d3:94:5d:ed:21:43:c1:e6:c8:e2:a6:06:73:e9:88:79:ff:c
                    0:2a:4a:7d:71:2d:77:23:13:a6:11:b7:a0:e7:23:19:27:89:b9:f2:73:32:26:88:70:82:b3:3f:7d:5d:4e:51:32:f0:b3:8c:d
                    3:2c:25:59:9d:54:9b:21:3f:0a:26:67:86:6c:9d:c4:94:ad:aa:f0:3b:ec:af:2e:a9:1a:58:7b:49:70:83:fb:71:c8:fb:b8:f5:
                    47:4d:5d:a5:9c:95:0a:b4:e1:ac:78:41:af:72:7a:8c:f2:53:f7:95:9f:83:89:4f:80:ab:6f:20:e6:c5:e0:8c:53:5a:1b:2e:20
                    :f2:7a:b3:2b:9f:31:dc:df:de:37:32:ee:8a:f6:27:37:00:aa:dd:a5:b9:16:b6:31:7b:59:8d:f7:09:77:41:bb:93:b1:87:e6:
                    53:7a:78:06:1d:dd:81:51:cb:74:18:07:f5:f0:b0:ec:f9:84:db:b8:c3:ac:3c:8b:bf:cc:2b:b3:6e:d6:52:ad:1c:ce:99:c1:93
                    :2e:44:e5:66:78:e3:b1:96:f7:75:fa:f6:3e:f0:aa:e5:c0:77:ef:db:61:ac:27:6a:e3:bd:4d:d8:1d:7f:16:17:56:0a:31:a6:2
                    6:0b:68:2b:72:e7:17:fc:46:8b:18:1b:db:8d:9e:ae:ea:3a:37:a3:e4:5d:19:e9:e8:1d:15:d8:5c:9a:00:78:54:87:a1:ee:a
                    e:22:1b:2a:1f:b3:44:5d:ef:1e:71:fa:1f:74:14:62:44:90:dc:cf:9c:db:74:b0:2d:5b:9f:9c:8e:b1:d3:ff:59:67:ff:5c:4e:a1
                    :76:be:7a:7f:f7:3a:3e:05:6c:78:f2:fd:4a:c7:75:bf:08:cc:25:ab:8b:f2:84:6e:15:61:ce:64:8f:a3:b7:90:cf:47:62:d6:89

                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                OCSP - URI:http://ocsp.ncdc.gov.sa
                CA Issuers - URI:http://web.ncdc.gov.sa/certs/snrcasha256.crt

            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://www.ncdc.gov.sa

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://web.ncdc.gov.sa/crl/nrcaparta1.crl
                  DirName:C = SA, O = National Center for Digital Certification, OU = Saudi National Root CA, CN = CRL1

                Full Name:
                  URI:http://web.ncdc.gov.sa/crl/nrcacomb1.crl

            X509v3 Authority Key Identifier:
                keyid:FC:99:98:41:17:E3:F3:3D:1E:FD:B7:72:A9:BF:A3:16:E4:2A:E9:AA

            X509v3 Subject Key Identifier:
                B4:37:78:F2:5E:40:16:2F:17:E3:12:32:A4:03:C6:AA:F8:43:0D:34
    Signature Algorithm: sha256WithRSAEncryption
        67:2f:af:d6:57:2e:0b:46:43:4e:6f:cf:da:ae:63:ce:ca:75:df:60:e6:1e:f0:ed:26:c1:fa:c2:74:0c:24:fd:2d:83:52:20:a9:91:b4:
        ed:4f:98:cb:12:8d:0e:b8:d3:21:7a:74:22:ac:7d:53:6e:c1:d6:ef:a6:00:6e:6f:d1:00:26:89:b1:4a:8a:f8:f5:31:8c:30:99:3a:9
        1:2d:10:07:89:6a:22:3e:6c:ad:97:8b:db:af:73:00:0f:8f:39:29:5c:b2:fe:44:dc:81:8e:d3:0c:52:1c:78:f1:3e:55:1f:30:cb:8d:
        96:a1:1a:33:2f:0f:e7:6b:0f:9b:fb:be:3e:fb:14:2c:32:e5:1e:61:72:88:cc:55:18:64:37:42:87:5a:5b:94:32:b2:98:28:7c:74:1
        d:93:16:b7:b5:ea:55:b4:01:24:34:d2:18:53:fa:42:1d:ce:a0:ee:54:b3:80:33:01:df:9a:12:4f:1a:dc:44:76:ad:f2:1a:79:5e:e8
        :56:08:39:8a:d7:93:a1:6f:40:1c:bb:7a:50:e4:6b:bc:e5:d8:1c:87:17:26:23:e7:10:84:b4:eb:1f:94:ea:49:10:4e:c2:98:57:b1
        :fd:1a:b5:a1:2b:50:95:71:08:b2:62:cf:f7:03:62:b5:e0:b9:9e:4b:0c:cc:f0:0c:8d
```

EMDHA eSign CA Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            32:c8:f7:71:ef:fd:f1:1f:cd:e7:d5:0c:ef:e7:eb:34
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = SA, O = Baud Telecom Company, CN = BTC Licensed CA
        Validity
            Not Before: Dec 16 13:50:19 2019 GMT
            Not After : Nov 27 13:50:19 2029 GMT
        Subject: C = SA, O = Baud Telecom Company, CN = EMDHA eSign CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:a4:5f:1b:fc:6b:c2:7c:df:0b:fa:c0:cd:aa:20:8c:b9:f1:44:94:8a:1a:be:5f:02:7d:10:12:de:0a:0f:62:78:fd:cf:9c:4a:
                    14:96:71:bf:3f:6a:0c:2f:8f:89:1d:f0:d8:36:fd:8e:4d:05:56:e0:8d:b0:95:b1:64:ac:23:f6:b7:ea:74:b5:88:1c:e6:14:c
                    2:73:64:90:51:45:7f:ec:b4:f2:c2:48:0c:a3:fb:03:8b:39:83:7d:c8:cd:68:88:c4:7e:02:ce:b0:5e:e6:64:21:04:63:e2:5
                    3:e7:77:6e:e1:a5:b7:95:a8:af:cd:08:78:16:0e:46:8b:5b:6c:da:ac:79:97:97:af:86:b2:a4:3d:75:bf:71:b3:92:e8:67:d
                    5:85:27:fc:46:5b:f9:e1:60:c6:18:6b:6c:34:6e:98:51:a1:d1:56:af:0a:29:58:59:1a:87:8e:32:be:d5:ab:d5:8a:f5:a0:1
                    c:19:9e:ff:40:52:6d:af:3a:66:d4:15:65:a3:50:a9:f3:eb:93:1c:7d:b2:0c:e8:e9:de:76:dd:b8:54:6a:a8:77:e8:cb:b9:0
                    3:ef:99:82:5b:b0:43:49:ae:55:14:ac:94:cd:47:89:17:de:f9:b1:d8:89:7f:7c:a6:39:36:4b:e0:12:04:fb:7f:13:7a:e9:d
                    e:9d:ba:7e:55:39:41:03:61:fe:31:97:bb:ed:29:01:9a:5c:cf:13:51:9b:7e:5a:d7:4f:5d:6f:c1:5d:a9:9d:5f:ee:2b:5b:f3
                    :15:6a:08:39:40:60:44:e8:d4:aa:74:51:50:0d:b3:fc:72:22:d2:57:3b:2e:7c:4c:b8:7a:15:44:82:8a:dc:ca:94:9a:99:2
                    5:39:0f:34:87:60:f1:5b:df:02:26:42:f9:a6:24:16:29:49:23:94:2a:ca:70:5b:df:9c:d2:86:03:58:99:f1:51:29:8b:38:2
                    7:a5:85:01:24:51:fc:ca:42:99:de:00:a3:82:92:92:fd:b4:34:3d:be:31:3a:1d:5b:4e:6c:54:00:77:a0:d0:9c:35:e3:2d:
                    8c:74:46:e8:14:3b:0a:ca:82:03:c6:0e:cb:ac:82:d2:7e:06:82:a9:d1:68:88:f1:6a:6b:ab:e2:2e:f4:ac:21:9f:6f:9b:5c:3
                    1:bb:36:f5:80:e2:d4:73:40:aa:89:35:0d:f5:ce:f7:3d:26:58:61:b7:ea:9e:a8:c3:8b:61:45:91:36:e9:c4:39:6e:f6:51:b
                    d:63:32:be:da:a1:38:77:66:30:ab:d7:9a:16:c6:a0:68:49:50:cc:64:3b:25:d8:e8:34:6b:3d:d8:bc:c4:7c:a6:aa:59:9a:
                    80:e3:12:25:d2:e2:8a:49
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            Authority Information Access:
                CA Issuers - URI:http://repository.emdha.sa/cacerts/L1CA19.crt
                OCSP - URI:http://ocsp.emdha.sa

            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://www.emdha.sa
                  User Notice:
                    Explicit Text:

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://repository.emdha.sa/crls/L1CA19.crl

            X509v3 Authority Key Identifier:
                keyid:B4:37:78:F2:5E:40:16:2F:17:E3:12:32:A4:03:C6:AA:F8:43:0D:34

            X509v3 Subject Key Identifier:
                04:93:7B:60:34:A9:B4:B8:28:28:F0:FF:43:AA:56:D1:94:ED:A4:CC
    Signature Algorithm: sha256WithRSAEncryption
        25:d5:82:e9:6e:f3:6d:97:6a:43:71:37:32:47:04:4a:b6:0e:38:37:96:37:10:26:18:d7:80:c3:51:f5:49:db:20:be:51:0f:dc:db:
        5c:b6:02:73:df:0c:52:7a:a1:28:37:a5:9f:c5:4a:5a:9b:4a:57:26:61:4c:71:f9:6a:c7:0f:9f:dd:c9:17:f1:5d:5c:35:8e:e0:25:88
        :ca:33:89:48:9d:7f:65:6e:b6:9a:82:d4:27:17:10:02:b3:a5:5a:e4:33:14:45:1d:6d:3b:99:8f:ab:02:a5:f3:ad:c5:15:d6:23:43
        :07:4d:a6:3c:d1:8a:89:66:3b:72:48:43:82:90:44:39:8a:11:cf:ff:7d:5c:2c:bb:91:4b:ee:ae:d2:d9:4a:32:99:8c:5f:f8:a2:fd:a
        0:c4:6e:3e:29:ba:03:72:dd:0c:65:cb:c7:67:9e:2a:8b:cb:b9:f2:95:7c:d1:ea:8d:67:fd:34:55:e0:90:fd:31:e3:33:2a:59:40:9f
        :bd:1f:ac:57:b8:76:10:35:5b:45:30:f9:2a:fb:cb:15:09:e6:2e:6f:bb:1f:21:af:fb:08:02:8a:a8:49:f4:80:85:95:c7:ac:b4:e2:b5
        :e2:e4:57:32:33:54:d8:4a:8a:f9:98:fd:9b:3b:4e:1d:1d:ee:ab:66:eb:46:11:20:83:b8:84:47:85:21:33:38:a4:1d:c1:28:e7:ae
        :b5:90:32:87:8d:13:00:42:89:03:7b:88:c8:6f:54:ec:e9:61:bc:8e:2a:54:36:ab:69:98:68:5f:97:35:00:10:16:ab:c8:f7:dc:dd:
        1f:98:60:01:70:fd:f3:ae:e7:69:9d:a0:3a:5e:56:2b:ff:7d:65:26:41:37:bc:83:01:f8:f7:df:4c:69:95:8b:c7:d9:7b:8e:9e:c3:9d:
        d7:43:44:c4:b0:22:ff:7c:c6:be:fc:82:f8:48:f3:5d:e7:92:44:52:9a:8b:a5:b2:13:90:cc:de:68:bc:3a:ae:c5:0c:f7:a0:c1:4a:c8:
        91:87:09:3e:e1:f3:0b:0b:9f:e3:4f:48:fe:fa:f0:e8:e6:a4:e6:9a:40:a1:80:3b:01:28:88:fe:48:30:0e:ee:b4:63:98:bd:44:02:f1
        :7a:98:1f:69:b8:cd:41:3b:13:ae:c7:1b:35:a3:ba:b7:6e:28:10:05:ee:23:40:22:49:c1:39:75:8c:be:a4:49:e3:c0:8c:62:e3:66
        :6a:9b:f4:6a:7b:33:63:3b:a2:ec:c2:e0:e2:24:10:85:dd:b8:cf:cd:e2:81:35:75:33:0c:5d:46:4c:cb:86:fa:13:0c:04:da:f9:48:9
        3:81:9c:06:ec:da:77:21:2b:32:f1:c7
```

Baud Telecom Company Management's Assertion

Baud Telecom Company ("BTC") has deployed a public key infrastructure. As part of this deployment, it was necessary to create a hierarchy of Certificate Authorities (CAs) consisting of:

1. BTC Licensed CA
2. EMDHA eSign CA

These CAs will serve as Intermediate and Issuing CAs for client certificate services. In order to allow the CA to be installed in a final and useable configuration, a Key Generation Ceremony was conducted, the purpose of which was to formally witness and document the creation of the CA's signing private key. This helps assure the non-refutability of the integrity of the BTC Licensed CA and EMDHA eSign CA key pairs, and in particular, the signing private keys.

BTC management has securely generated the key pairs, consisting of a public and private keys, in support of its CA operations. The key pairs were generated in accordance with procedures described in BTC's Certificate Policy/Certificate Practice Statement (CP/CPS) and its Key Generation Script.

BTC 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 key generation process.

BTC management is responsible for:

- Establishing and maintaining procedures over its BTC Licensed CA and EMDHA eSign CA key generation;
- Implementing effective controls over its CA key generation process and the integrity and confidentiality of all private keys and access keys, (including physical keys, tokens, and passwords) used in the establishment of BTC Licensed CA and EMDHA eSign CA ; and
- Implementing CA environmental controls relevant to the generation and protection of their CA keys.

BTC management has assessed the procedures and controls for the generation of the CA keys. Based on that assessment, in management's opinion, in generating and protecting its CA keys for the BTC Licensed CA and EMDHA eSign CA, on 16 December 2019 in Riyadh, Kingdom of Saudi Arabia, with the following identified information:

CA Name	Subject Key Identifier	Certificate Serial Number	SHA Fingerprint
BTC Licensed CA	b4 37 78 f2 5e 40 16 2f 17 e3 12 32 a4 03 c6 aa f8 43 0d 34	00db0e7b442047c265000000005c5228e2	B0:D8:31:88:C1:5A:95:BE:4B:82:5E:A4:17:B1:2C:ED:62:39:F8:BD:53:21:90:47:CE:89:08:12:55:F3:01:CC
EMDHA eSign CA	04 93 7b 60 34 a9 b4 b8 28 28 f0 ff 43 aa 56 d1 94 ed a4 cc	32c8f771effdf11fcde7d50cefe7eb34	1C:F1:83:8F:F6:28:48:46:6F:2F:BF:15:98:25:8B:45:1D:39:4F:C6:F4:A2:0D:BF:70:29:C1:BF:43:A7:1C:BA

BTC has:

- Followed the CA key generation and protection requirements of the BTC Licensed CA CP/CPS, version 1.0, dated 12 December 2019;
- Included appropriate, detailed procedures and controls in its Key Generation Script:
  - BTC Licensed CA and EMDHA eSign CA, dated 12 December 2019;
- Maintained effective controls to provide reasonable assurance that the CA was generated and protected in conformity with the procedures described in its CP/CPS and its Key Generation Script;
- Performed, during the CA keys generation process, all procedures required by the Key Generation Script;
- Generated the CA keys in a physically secured environment as described in its CP/CPS;
- Generated the CA keys using personnel in trusted roles under multiple person control and split knowledge;
- Generated the CA keys within hardware cryptographic module (SafeNet Luna S750, firmware version 7.3.3) meeting the applicable technical and business requirements as disclosed in its CP/CPS.

Ibrahim Alkharboush

Policy Authority Committee
Digitally signed by Policy Authority Committee
Date: 2020.01.26 17:11:33 +03'00'

Senior Vice President
Baud Telecom Company
20 January 2020