bsi.

...making excellence a habit.™

EBG Bilisim Teknolojileri ve Hizmetleri A.S
Attn.: Mr. H. Kuran
Ceyhun Atıf Kansu, Cad. 130
58 Balgat / ANKARA
TURKEY

Amsterdam, 22 April 2013

Subject: Observations of the E-Tugra Key Ceremony held on 5 March 2013

Dear Mr. Kuran,

On the request of EBG Bilisim Teknolojileri ve Hizmetleri A.S (hereafter: E-Tugra), we witnessed and observed the key ceremony held on 5 March 2013 at the E-Tugra offices in Ankara. During this ceremony, one root CA-certificate and three sub CA-certificates were generated:

- E-Tugra Certification Authority (Root);
  - E-Tugra Organization Validated CA;
  - E-Tugra Domain Validated CA; and
  - E-Tugra Extended Validated CA.

Key ceremony findings

The ceremony resulted in the correct generation of the certificates, according to a controlled Key Generation Script and in accordance with the audit frameworks ETSI TS 102042 v2.3.1 (section 7.2) and the CA/Browser Forum's Baseline Requirements, v1.1 (section 17.7). The controls used to ensure the integrity and confidentiality of the key pair are considered to be effective.

Our detailed findings and observations of the ceremony are outlined below:

- The key ceremony was performed in a secure server room. This room is protected by five physical zones, including three zones requiring dual access and one zone enforcing physical access by a circular gate. At all times, at least three persons in trusted roles attended the ceremony. The ceremony was recorded on video and was performed in presence of an external auditor and an external legal witness.
- The key pairs were generated in a HSM, certified according to FIPS PUB 140-2 level 3. The root CA key pair was generated with the combination of the sha256 RSA algorithm using a 4096 bit length. The sub-CAs are generated using the same algorithms, using a 2048 bit length. These combinations are recognized by the industry as being fit for purpose for CA's signing operations.

Adam Smith Building
Thomas R. Malthusstraat 3c
1066 JR Amsterdam
The Netherlands

P.O. Box 74103
1070 BC Amsterdam
The Netherlands

T: +31 20 346 0780
F: +31 20 346 0781
info.nl@bsigroup.com
bsigroup.nl

- The Primekey EJBCA software used to generate the CA certificates is version 5.0.8. Primekey EJBCA version 5.0.4 has certified against EAL4+. The change log specifying the changes from version 5.0.4 through version 5.0.8. was published on the Primekey website on 19 December 2012 and contains maintenance releases only, mainly concerning security improvements and bug fixes. The difference in the certified EJBCA version and implemented version by E-Tugra is considered to be adequately accounted for.
- During the key ceremony, E-Tugra has created back-ups of the-CA keys on smartcards. The smartcards are certified against Common Criteria v2.1, the related report is issued on 20 May 2005. The smartcards are archived in separate parts in three bank vaults. The keys owned by E-Tugra to open the bank vaults are stored under dual control. Only the E-Tugra CEO is authorised to access the bank vaults (together with a bank employee). The smartcards and passwords are stored in regular envelopes. In order to restore the CA key, three custodians are required and the smartcards should be retrieved from (at least) two bank vaults. In general, this is considered to provide adequate protection and restore capability.
- E-Tugra has adequately documented minor deviations and/or additions to the key ceremony procedure in an appendix. A CA-key pair slot in the HSM which inadvertently became inaccessible during the ceremony was destroyed the next business day. No CA certificate was generated based on the key pair stored in this slot, therefore archiving of this key pair was not needed.

Distribution of this letter

BSI grants permission to distribute a copy of this letter upon request and only to the designated contact persons at the following organisations:

- Mozilla Foundation
- Microsoft
- Google
- Opera
- Apple

e-Tugra and each of the designated persons at the above mentioned organisations will not further distribute the letter, including by disclosing it to the public through physical or electronic means. Notwithstanding the foregoing, upon explicit request of Mozilla, the contact person at Mozilla may disclose the letter on Mozilla's Bugzilla.

BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with the purpose for which this letter may be used, or to whom the letter is disclosed.

BSI, its staff and agents shall keep confidential all information relating to e-Tugra and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

Please do not hesitate to contact us, should you have any questions with regard to this letter.

Sincerely yours,

On behalf of BSI Group The Netherlands B.V.

Drs. Dave T.P. Hagenaars
Managing Director