Report on Management's Assertion Related to the Key Transference of GlobalSign Root R2 and GlobalSign Root R4

Google Trust Services LLC

As of November 17, 2016

Building a better
working world

Report on Management’s Assertion Related to the Key Transference of GlobalSign Root R2 and GlobalSign Root R4

Table of contents

Building a better
working world

Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5553
Fax: +1 408 947 5717
ey.com

INDEPENDENT ACCOUNTANT'S REPORT

To the management of Google Trust Services LLC:

We have examined Google Trust Services LLC ("GTS") Management's Assertion that in transferring its GlobalSign Root R2 and GlobalSign Root R4 (collectively, "Google Root CAs") from GMO GlobalSign, Inc.'s ("GlobalSign") facilities in Singapore to GTS' Google Internet Authority ("GIA") G2 Certification Authority facilities in Zurich, Switzerland, and Mountain View, California on August 11, 2016 with the following identifying information:

Root Name	**Subject Key Identifier**	**Certificate Serial Number**
GlobalSign Root R2	75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe	04:00:00:00:00:01:0f:86:26:e6:0d
GlobalSign Root R4	69:69:56:2e:40:80:f4:24:a1:e7:19:9f:14:ba:f3:ee:58:ab:6a:bb	2a:38:a4:1c:96:0a:04:de:42:b2:28:a5:0b:e8:34:98:02

GTS has:

- exported the private keys within a secure key management scheme as encrypted key fragments using multiple control and split knowledge; and

- secured and tracked the private keys for movement from the GlobalSign facilities in Singapore to GTS' GIA G2 facilities in Zurich, Switzerland, and Mountain View, California on August 11, 2016

based on the Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, and Key Storage, Backup and Recovery Criterion 4.2 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

GTS' management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of GTS' documented plan of procedures to be performed for the transference of the certification authority key pairs for the Google Root CAs;

(2) reviewing the detailed CA key transference script for conformance with industry standard practices;

(3) testing and evaluating, during the CA key transference process, the effectiveness of controls over the integrity and confidentiality of all private keys, including back-up copies, and access keys (including physical keys, tokens, and passwords);

(4) physical observation of all procedures performed during the root key transference process to ensure the procedures actually performed on August 11, 2016 were in accordance with the Root Key Transference Script(s) for the Google Root CAs; and

(5) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination procedures provides a reasonable basis for our opinion.

In our opinion, as of November 17, 2016, Google Trust Services LLC Management’s Assertion, as referred to above, is fairly stated, in all material respects, based on Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, and Key Storage, Backup and Recovery Criterion 4.2 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

This report does not include any representation as to the quality of GTS’ services beyond those covered by Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2 and Key Storage, Backup and Recovery Criterion 4.2 of the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of GTS’ services for any customer's intended purpose.

This report is intended solely for the information and use of Google management, representatives of the browsers, and representatives of the trust stores, and should not be used by anyone other than these specified parties.

Ernst + Young LLP

November 18, 2016

1600 Amphitheatre Parkway
Mountain View, California 94043

Google

Tel: 650.253.0000
www.google.com

Google Trust Services LLC

Google Trust Services LLC MANAGEMENT'S ASSERTION

Google Trust Services LLC ("GTS") has deployed a public key infrastructure. As part of this deployment, it was necessary to obtain self-signed Root CAs known as GlobalSign Root R2 and GlobalSign Root R4 (collectively, "Root CAs"). A Key Transference Ceremony was conducted to transfer possession of the Root CAs from GMO GlobalSign, Inc.'s ("GlobalSign") facilities in Singapore to GTS' Google Internet Authority ("GIA") G2 Certification Authority facilities in Zurich, Switzerland and Mountain View, California, and to validate the chain of custody of the Root CAs' key pairs from GlobalSign to GTS.

GTS management has securely exported the Root CAs key pairs, each consisting of a public and private key, within a secure key management scheme as encrypted key fragments using multiple control and split knowledge which were then tracked for movement from GlobalSign's facilities to GTS' facilities in accordance with procedures described in its Certification Practice Statement ("CPS") and its Key Transference Script dated August 11, 2016, which is based on the Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, and Key Storage, Backup and Recovery Criterion 4.2 of the WebTrust Principles and Criteria for Certification Authorities v2.0. We also acknowledge that we are responsible for determining that such aforementioned criteria are appropriate for its purposes.

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

GTS management is responsible for establishing and maintaining procedures over the integrity and confidentiality of all private keys and access keys (including physical keys, tokens, and passwords) used in the establishment of the Root CAs, and for the CA environment controls relevant to the security of its CA keys.

GTS management has assessed the procedures and controls for the storage and asset management of the CA keys. Based on that assessment, in management's opinion, in securing its CA keys for the Root CAs and the transference of the Root CAs from GlobalSign's facilities in Singapore to GTS' GIA G2 Certification Authority facilities in Zurich, Switzerland, and Mountain View, California on August 11, 2016 with the following identifying information:

Root Name	**Subject Key Identifier**	**Certificate Serial Number**
GlobalSign Root R2	75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe	04:00:00:00:00:01:0f:86:26:e6:0d
GlobalSign Root R4	69:69:56:2e:40:80:f4:24:a1:e7:19:9f:14:ba:f3:ee:58:ab:6a:bb	2a:38:a4:1c:96:0a:04:de:42:b2:28:a5:0b:e8:34:98:02

GTS has:

- exported the private keys within a secure key management scheme as encrypted key fragments using multiple control and split knowledge; and
- secured and tracked the private keys for movement from the GlobalSign facilities in Singapore to GTS' GIA G2 facilities in Zurich, Switzerland, and Mountain View, California on August 11, 2016

based on the Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, and Key Storage, Backup and Recovery Criterion 4.2 of the WebTrust Principles and Criteria for Certification Authorities v2.0.

GOOGLE TRUST SERVICES LLC
November 18, 2016