# Report on Management's Assertion Related to the Key Generation and Key Transference of GTS Root R1, GTS Root R2, GTS Root R3, and GTS 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 Generation and Key Transference of GTS Root R1, GTS Root R2, GTS Root R3, and GTS Root R4

## Table of contents

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

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

Building a better working world

# 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 generating and securing its GTS Root R1, GTS Root R2, GTS Root R3, and GTS Root R4 (collectively, "Google Root CAs") on June 22, 2016 in Singapore, and the subsequent transference of the 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 |
|---|---|---|
| GTS Root R1 | e4:af:2b:26:71:1a:2b:48:27:85:2f:52:66:2c:ef:f0:89:13:71:3e | 6e 47 a9 c5 4b 47 0c 0d ec 33 d0 89 b9 1c f4 e1 |
| GTS Root R2 | bb:ff:ca:8e:23:9f:4f:99:ca:db:e2:68:a6:a5:15:27:17:1e:d9:0e | 6e 47 a9 c6 5a b3 e7 20 c5 30 9a 3f 68 52 f2 6f |
| GTS Root R3 | c1:f1:26:ba:a0:2d:ae:85:81:cf:d3:f1:2a:12:bd:b8:0a:67:fd:bc | 6e 47 a9 c7 6c a9 73 24 40 89 0f 03 55 dd 8d 1d |
| GTS Root R4 | 80:4c:d6:eb:74:ff:49:36:a3:d5:d8:fc:b5:3e:c5:6a:f0:94:1d:8c | 6e 47 a9 c8 8b 94 b6 e8 bb 3b 2a d8 a2 b2 c1 99 |

GTS has:

- followed the CA key generation and security requirements in its:
  - Google Internet Authority G2 CPS v1.4
- included appropriate, detailed procedures and controls in its Root Key Generation Script on June 22, 2016;
- maintained effective controls to provide reasonable assurance the Google Root CAs were generated and secured in conformity with the procedures described in its Certification Practices Statement ("CPS") and its Root Key Generation Script;
- performed, during the root key generation process, all procedures required by the Root Key Generation Script;
- 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;

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

- stored the generated CA keys between June 22, 2016 and August 11, 2016 in the GlobalSign facility and stored them in such a way that neither party alone could utilize the materials; and

- secured and tracked the generated CA 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 Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, CA Key Generation Criterion 4.1, 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 generation and transference of the certification authority key pairs for the Google Root CAs;

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

(3) testing and evaluating, during the CA key generation and 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 generation process to ensure the procedures actually performed on June 22, 2016 were in accordance with the Root Key Generation Script for the Google Root CAs;

(5) validating the key material was secured for the period between June 22, 2016 and August 11, 2016 while at the GlobalSign facilities;

(6) validating the key material was fragmented using multiple control and split ownership between GlobalSign and GTS in such a way that neither party could utilize the materials for the period between June 22, 2016 and August 11, 2016;

(7) 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

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

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

Building a better working world

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, CA Key Generation Criterion 4.1, 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, CA Key Generation Criterion 4.1, 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 create a hierarchy consisting of self-signed Root CAs known as GTS Root R1, GTS Root R2, GTS Root R3, and GTS Root R4 (collectively, "Google Root CAs"). These CAs will serve as Root CAs for GTS certificate services. To allow the CAs to be installed in a final production configuration, a Root Key Generation Ceremony was conducted in GMO GlobalSign, Inc.'s ("GlobalSign") facilities in Singapore, the purpose of which was to formally witness and document the creation of the CAs' private signing key and assure the non-refutability of the integrity of the Google Root CAs' key pairs, and in particular, the private signing keys. A Key Transference Ceremony was then conducted to transfer possession of the root keys from the GlobalSign facilities in Singapore to GTS' Google Internet Authority ("GIA") G2 Certification Authority facilities in Zurich, Switzerland and Mountain View, California, to validate the chain of custody of the Google Root CAs' key pairs from GlobalSign to GTS.

GTS management has securely generated key pairs, each consisting of a public and private key, in support of its CA operations and then securely exported the key pairs within a secure key management scheme as encrypted key fragments using multiple control and split knowledge that were then tracked for movement from GMO GlobalSign, Inc.'s facilities to GTS' facilities. The key pairs were generated, secured, and tracked for movement in accordance with procedures described in GTS' Certification Practice Statement ("CPS"), its Root Key Generation Script dated June 22, 2016, and its Key Transference Script dated August 11, 2016, which were based on Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, CA Key Generation Criterion 4.1, 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 generation, 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 generation process.

GTS 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 Google Root CAs, and for the CA environment controls relevant to the generation and security of its CA keys.

GTS 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 securing its CA keys for the Google Root CAs on June 22, 2016 at Singapore, and the subsequent transference of the Google 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 |
|---|---|---|
| GTS Root R1 | e4:af:2b:26:71:1a:2b:48:27:85:2f:52:66:2c:ef:f0:89:13:71:3e | 6e 47 a9 c5 4b 47 0c 0d ec 33 d0 89 b9 1c f4 e1 |
| GTS Root R2 | bb:ff:ca:8e:23:9f:4f:99:ca:db:e2:68:a6:a5:15:27:17:1e:d9:0e | 6e 47 a9 c6 5a b3 e7 20 c5 30 9a 3f 68 52 f2 6f |
| GTS Root R3 | c1:f1:26:ba:a0:2d:ae:85:81:cf:d3:f1:2a:12:bd:b8:0a:67:fd:bc | 6e 47 a9 c7 6c a9 73 24 40 89 0f 03 55 dd 8d 1d |
| GTS Root R4 | 80:4c:d6:eb:74:ff:49:36:a3:d5:d8:fc:b5:3e:c5:6a:f0:94:1d:8c | 6e 47 a9 c8 8b 94 b6 e8 bb 3b 2a d8 a2 b2 c1 99 |

GTS has:

- followed the CA key generation and security requirements in its:
    - Google Internet Authority G2 CPS v1.4
- included appropriate, detailed procedures and controls in its Root Key Generation Script on June 22, 2016;
- maintained effective controls to provide reasonable assurance the Google Root CAs were generated and secured in conformity with the procedures described in its Certification Practices Statement (CPS) and its Root Key Generation Script;
- performed, during the root key generation process, all procedures required by the Root Key Generation Script;
- 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;
- exported the private keys within a secure key management scheme as encrypted key fragments using multiple control and split knowledge;
- stored the generated CA keys between June 22, 2016 and August 11, 2016 in the GlobalSign facility and stored them in such a way that neither party alone could utilize the materials; and
- secured and tracked the generated CA 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 Certification Practices Statement Management Criterion 2.2, Asset Classification and Management Criterion 3.2, CA Key Generation Criterion 4.1, 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