

## Report of Independent Accountants

To the Management of Google Trust Services LLC:

We have examined the accompanying [assertion](#) made by the management of Google Trust Services LLC ("GTS") that in providing its Certification Authority (CA) services at Mountain View, California and Zurich, Switzerland for the Root and Subordinate CAs referenced in **Appendix A** during the period from August 11, 2016 through August 10, 2017, GTS has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its:

For the period August 11, 2016 to December 8, 2016:

- Google Internet Authority G2 [Certification Practice Statement v1.4](#)

For the period December 9, 2016 to August 10, 2017

- Google Trust Services [Certification Practice Statement v1.9](#)
- Google Trust Services [Certificate Policy v1.3](#)

- maintained effective controls to provide reasonable assurance that:
  - GTS' Certificate Practice Statement was consistent with its Certificate Policy
  - GTS provided its services in accordance with its Certificate Policy and Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - subscriber information was properly authenticated (for the registration activities performed by GTS); and
  - the integrity of subscriber keys and certificates it managed was established and protected throughout their lifecycles;
  - subordinate CA certificate requests are accurate, authenticated, and approved
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

based on the American Institute of Certified Public Accountants (AICPA)'s [Trust Services Principles and Criteria for Certification Authorities 2.0](#).

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

GTS does not escrow its CA keys, does not provide subscriber key storage and recovery services, does not support ICC life cycle management, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of GTS' key and certificate life cycle management business practices, policies, processes and controls, and its suitability of the design and implementation of the controls intended to achieve the Criteria and examining evidence supporting management's assertion and performing such other procedures over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance and operation of systems integrity as we considered necessary in the circumstances; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at GTS and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Our examination was not conducted for the purpose of evaluating GTS' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, GTS may achieve reasonable, but not absolute assurance that all security events are prevented and, for those controls may provide reasonable, but not absolute assurance that its commitments and system requirements are achieved. Controls may not prevent or detect and

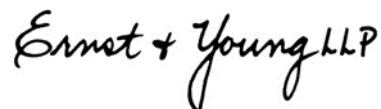
correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, the projection of any evaluations of effectiveness to future periods is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

In our opinion, GTS' management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria.

The WebTrust seal of assurance for Certification Authority on GTS' website constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

This report does not include any representation as to the quality of GTS' CA services beyond those covered by the [Trust Services Principles and Criteria for Certification Authorities Version 2.0](#) criteria, or the suitability of any of GTS' services for any customer's intended purpose.



San Jose, California  
November 1, 2017



## Google Trust Services LLC

### **Management's Assertion Regarding the Effectiveness of Its Controls Over Certificate Authority Operations Based on the Trust Services Principles and Criteria for Certification Authorities Version 2.0**

November 1, 2017

We, as management of, Google Trust Services LLC ("GTS") are responsible for operating a Certification Authority (CA) at Mountain View, California and Zurich, Switzerland for the Root and Subordinate CA's listed in **Appendix A**.

GTS' CA services provide the following certification authority services:

- Subscriber key generation and management
- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

The management of GTS is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to GTS' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of GTS has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in GTS Management's opinion, in providing its CA services for the Root and Subordinate CA's listed in **Appendix A** at Mountain View, California and Zurich, Switzerland during the period from August 11, 2016 through August 10, 2017, GTS has:

- disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its:

For the period August 11, 2016 to December 8, 2016:

- Google Internet Authority G2 [Certification Practice Statement v1.4](#)



## Google Trust Services LLC

For the period December 9, 2016 to August 10, 2017

- Google Trust Services [Certification Practice Statement v1.9](#)
- Google Trust Services [Certificate Policy v1.3](#)
  
- maintained effective controls to provide reasonable assurance that:
  - GTS' Certificate Practice Statement was consistent with its Certificate Policy
  - GTS provided its services in accordance with its Certificate Policy and Certification Practice Statement
  
- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - subscriber information was properly authenticated (for the registration activities performed by GTS); and
  - the integrity of subscriber keys and certificates it managed was established and protected throughout their lifecycles
  - subordinate CA certificate requests are accurate, authenticated, and approved
  
- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity

for the Root and Subordinate CA's listed in **Appendix A**, based on the [Trust Services Principles and Criteria for Certification Authorities Version 2.0](#), including the following:

### **CA Business Practices Disclosure**

CA Business Practices Disclosure  
Certification Practice Statement (CPS)  
Certificate Policy (CP)

CA Business Practices Management  
Certificate Policy Management  
Certification Practice Statement Management  
CP and CPS Consistency

### **Service Integrity**

CA Key Life Cycle Management Controls  
CA Key Generation  
CA Key Storage, Backup, and Recovery  
CA Public Key Distribution  
CA Key Usage  
CA Key Archival and Destruction



## Google Trust Services LLC

CA Key Compromise  
CA Cryptographic Hardware Life Cycle Management

Subscriber Key Life Cycle Management Controls  
CA Provided Subscriber Key Generation Services  
Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls  
Subscriber Registration  
Certificate Renewal  
Certificate Rekey  
Certificate Issuance  
Certificate Distribution  
Certificate Revocation  
Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls  
Subordinate CA Certificate Lifecycle Management

### **CA Environmental Controls**

Security Management  
Asset Classification and Management  
Personnel Security  
Physical and Environmental Security  
Operations Management  
System Access Management  
Systems Development and Maintenance  
Business Continuity Management  
Monitoring and Compliance  
Audit Logging

**GOOGLE TRUST SERVICES LLC**

## Appendix A

| Root/Subordinate CA 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 X1                           | 10:0a:72:b4:18:60:9b:33:69:e4:fe:8b:b0:df:d2:0d:8b:d8:e5:53 | 6e:47:a9:c9:a5:53:e3:c2:ce:1f:14:4e:d7:7d:ac:e7    |
| 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 X2                           | 0a:88:47:41:60:20:4c:ab:69:09:1e:ae:b4:66:8b:35:1f:65:b9:67 | 6e:47:a9:ca:ce:7f:84:65:19:2e:e7:33:2b:27:27:c3    |
| 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 X3                           | 9f:98:b3:74:b5:17:3c:32:3a:fe:f4:f6:64:b1:b1:68:c3:80:c0:5a | 6e:47:a9:cc:b4:5a:29:c7:b0:78:d0:1b:a3:21:12:61    |
| 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 X4                           | fe:9c:9c:0e:77:c1:48:11:0d:7c:19:0a:25:d5:e2:ab:64:57:df:65 | 6e:47:a9:ce:4f:46:c2:3d:e2:49:ea:cc:38:94:53:73    |
| 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                   |
| • Google Internet Authority G3     | 77:c2:b8:50:9a:67:76:76:b1:2d:c2:86:d0:83:a0:7e:a6:7e:ba:4b | 30:12:9b:fd:80:d1:93:d6:b3:e2:34:e4                |
| • Google Internet Authority G3     | 77:c2:b8:50:9a:67:76:76:b1:2d:c2:86:d0:83:a0:7e:a6:7e:ba:4b | 01:e3:a9:30:1c:fc:72:06:38:3f:9a:53:1d             |
| • GTS CA 1O1                       | 98:d1:f8:6e:10:eb:cf:9b:ec:60:9f:18:90:1b:a0:eb:7d:09:fd:2b | 01:e3:b4:9a:a1:8d:8a:a9:81:25:69:50:b8             |
| • GTS CA 1D2                       | b1:dd:32:5d:e8:b7:37:72:d2:ce:5c:ce:26:fe:47:79:e2:01:08:e9 | 01:e3:b4:9d:77:cd:f4:0c:06:19:16:b6:e3             |
| 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 |
| • Google Internet Authority G3 ECC | 64:b8:34:04:8e:de:e3:2a:54:39:a4:3e:c7:9b:d8:00:0f:0c:22:e4 | 01:e3:ae:80:26:db:5b:41:e2:56:c2:a3:51             |