Building a better
working world

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

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Google LLC:

We have examined the accompanying assertion made by the management of Google LLC ("Google"), titled *Management's Assertion Regarding the Effectiveness of Its Controls Over the SSL Certificate Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3* for Google's Certification Authority (CA) services at Mountain View, California and Zurich, Switzerland, throughout the period October 1, 2017 to September 30, 2018 for the subordinate CA as enumerated in **Appendix A**, under external Root CA, GeoTrust Global CA, Google has**:**

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Google Internet Authority G2, Certification Practices Statement v2.3

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Google website, and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by Google)
- Maintained effective controls to provide reasonable assurance that:
  - Logical and physical access to CA systems and data is restricted to authorized individuals;
  - The continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity
- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3* (Criteria).

Google 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.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform the 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. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, 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.

Google's Management has disclosed to us the attached comments (**Appendix B**) that have been posted publicly in the online forums of the CA/Browser Forum, as well as the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these comments in determining the nature, timing and extent of our procedures.

The relative effectiveness and significance of specific controls at Google 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 Google's 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, Google 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, Google’s management’s assertion referred to above is fairly stated, in all material respects, based on the aforementioned Criteria.

Google’s use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal 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 Google’s CA services beyond those covered by the *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3*, or the suitability of any of Google’s services for any customer's intended purpose.

Ernst + Young LLP

November 1, 2018

Google LLC
1600 Amphitheatre
Parkway
Mountain View, CA, 94043

650-253-0000 main
Google.com

Management's Assertion Regarding the Effectiveness of Its Controls Over the SSL Certificate Authority Services Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3

November 1, 2018

We, as the management of Google LLC ("Google"), are responsible for operating the SSL Certification Authority (CA) services at Mountain View, California and Zurich, Switzerland for the Subordinate CA under external Root CA, GeoTrust Global CA, in scope for SSL Baseline Requirements and Network Security Requirements listed at **Appendix A**.

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 Google's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of Google has assessed the disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Mountain View, California and Zurich, Switzerland throughout the period from October 1, 2017 through September 30, 2018, Google has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Google Internet Authority G2, Certification Practices Statement v2.3

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Google website, and provided such services in accordance with its disclosed practices

- Maintained effective controls to provide reasonable assurance that:
  - The integrity of keys and SSL certificates it manages was established and protected throughout their lifecycles; and
  - SSL subscriber information was properly authenticated (for the registration activities performed by Google)

- 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 are properly authorized and performed to maintain CA systems integrity

- Maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

for the Subordinate CA in scope for SSL Baseline Requirements and Network Security Requirements at **Appendix A**, based on the *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3*.

GOOGLE LLC

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA-256 Fingerprint
Google Internet Authority G2	4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:BA:5A:81:2F	01:00:21:25:88:B0:FA:59:A7:77:EF:05:7B:66:27:DF	9B:75:9D:41:E3:DE:30:F9:D2:F9:02:02:7D:79:2B:65:D9:50:A9:8B:BB:6D:6D:56:BE:7F:25:28:45:3B:F8:E9

Appendix B

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
1	An OCSP outage occurred for two days and six (6) hours during the period from January 19, 2018 to January 21, 2018 impacting Mozilla Firefox browser users with the opt-in "Hard-fail" behavior enabled for revocation checking. As the outage was within the requirement to update the OCSP responder at least every four (4) days, this did not impact Google's ability to meet the relevant WebTrust criteria.	**2.5.5** The CA maintains controls to provide reasonable assurance that the CA: • makes revocation information available via the cRLDistributionPoints and/or authorityInformationAccess certificate extensions for Subordinate CA and Subscriber Certificates in accordance with the SSL Baseline Requirements Section 7.1.2. • for high-traffic FQDNs, distributes its OCSP responses in accordance with SSL Baseline Requirements. **2.5.6** The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of Subscriber Certificates: o If the CA publishes a CRL, then the CA shall update and reissue CRLs at least once every seven (7) days, and the value of the nextUpdate field must not be more than ten (10) days beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol (OCSP) at least every four (4) days and OCSP responses must have a maximum	Mozilla Dev Security Policy Link

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
		expiration time of ten (10) days. • for the status of subordinate CA Certificates o The CA shall update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field must not be more than twelve months beyond the value of the thisUpdate field; and o The CA shall update information provided via an Online Certificate Status Protocol at least (i) every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate. • the CA makes revocation information available through an OCSP capability using the GET method for Certificates issued in accordance with the SSL Baseline Requirements.	