

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 Certificate Authority Operations Based on the WebTrust Principles and Criteria for Certification Authorities Version 2.1* for Google’s Certification Authority (CA) services at Mountain View, California and Zurich, Switzerland for the Subordinate CA referenced in **Appendix A**, under external Root CA, GeoTrust Global CA, during the period from October 1, 2017 through September 30, 2018. Google has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
 - Google Internet Authority G2, [Certification Practices Statement v2.3](#)
- Maintained effective controls to provide reasonable assurance that:
 - Google provides its services in accordance with its Certificate Practices Statement
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages is established and protected throughout their lifecycles; and
 - 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

based on the [WebTrust Principles and Criteria for Certification Authorities Version 2.1](#) (Criteria).

Google’s 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.

Google does not escrow its CA keys, does not provide subscriber key generation, does not provide subscriber key storage and recovery services, does not support integrated circuit card (ICC) life cycle management, does not provide certificate suspension services, and does not issue subordinate CAs. 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 Google's 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.

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

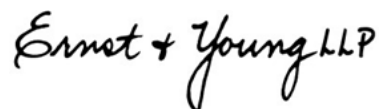
and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements.

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.

The WebTrust seal of assurance for Certification Authority on Google's 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 Google's CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities Version 2.1](#) criteria, or the suitability of any of Google's services for any customer's intended purpose.



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 Certificate Authority Operations
Based on the WebTrust Principles and Criteria for Certification Authorities Version 2.1**

November 1, 2018

We, as management of Google LLC ("Google"), are responsible for operating a Certification Authority (CA) at Mountain View, California and Zurich, Switzerland for the subordinate CA under the external Root CA, GeoTrust Global CA, listed in **Appendix A**.

Google's CA services provide the following certification authority services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation

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

Management of Google has assessed the disclosure of its certificate practices and its controls over its CA operations. Based on that assessment, in Google Management's opinion, in providing its CA services for the subordinate CA listed in **Appendix A** at Mountain View, California and Zurich, Switzerland during the period from October 1, 2017 through September 30, 2018, Google has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices as below:
 - Google Internet Authority G2, [Certification Practices Statement v2.3](#)

- Maintained effective controls to provide reasonable assurance that:
 - Google provides its services in accordance with its Certificate Practices Statement
- Maintained effective controls to provide reasonable assurance that:
 - The integrity of keys and certificates it manages was established and protected throughout their life cycles; and
 - The 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 were properly authorized and performed to maintain CA systems integrity

for the subordinate CA listed in **Appendix A**, based on the [WebTrust Principles and Criteria for Certification Authorities Version 2.1](#), including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certification Practice Statement Management

CA Environmental Controls

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

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction



- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Very truly yours,

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:B 6:BB:62:1A:BA:5A:8 1:2F	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:79:2 B:65:D9:50:A9:8B:BB:6 D:6D:56:BE:7F:25:28:4 5:3B: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.	<p>2.5.5 The CA maintains controls to provide reasonable assurance that the CA:</p> <ul style="list-style-type: none"> • 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. <p>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:</p> <ul style="list-style-type: none"> • for the status of Subscriber Certificates: <ul style="list-style-type: none"> ○ 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 ○ 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 expiration time of ten (10) days. • for the status of subordinate CA Certificates 	Mozilla Dev Security Policy Link

	Observation	Relevant WebTrust Criteria	Publicly Disclosed Link
		<ul style="list-style-type: none"> ○ 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 ○ 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. 	