Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110
Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Building a better working world

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"), 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 GTS' 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 October 1, 2017 through September 30, 2018. GTS has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - Google Trust Services, Certification Practices Statement v2.5; and
    - Google Trust Services, Certificate Policy v1.5
- Maintained effective controls to provide reasonable assurance that:
    - GTS' Certificate Practice Statement is consistent with its Certificate Policy; and
    - GTS provides 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 manages is established and protected throughout their lifecycles;
    - Subscriber information is properly authenticated (for the registration activities performed by GTS); and
    - 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 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).

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 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. 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.

GTS' 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 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

Building a better working world

internal control, GTS may achieve reasonable, but not absolute assurance that all security events are prevented and, 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 *WebTrust Principles and Criteria for Certification Authorities Version 2.1* criteria, or the suitability of any of GTS' services for any customer's intended purpose.

Ernst & Young LLP

November 30, 2018

1600 Amphitheatre Parkway
Mountain View, California 94043

Google

Tel: 650.253.0000
www.google.com

Google Trust Services LLC

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 30, 2018

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 registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subordinate CA certification

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, 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 October 1, 2017 through September 30, 2018, GTS has:

- Disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices as below:
    - Google Trust Services, Certification Practices Statement v2.5; and
    - Google Trust Services, Certificate Policy v1.5

- Maintained effective controls to provide reasonable assurance that:
    - GTS' Certificate Practice Statement is consistent with its Certificate Policy; and
    - GTS 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;
    - The Subscriber information was properly authenticated (for the registration activities performed by GTS); and
    - 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 *WebTrust Principles and Criteria for Certification Authorities Version 2.1*, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certification Practice Statement Management
- Certificate Policy Management
- CPS and CP Consistency

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Very truly yours,

GOOGLE TRUST SERVICES LLC

Appendix A

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
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	2A:57:54:71:E3:13:40:BC:21:58:1C:BD:2C:F1:3E:15:84:63:20:3E:CE:94:BC:F9:D3:CC:19:6B:F0:9A:54:72
• 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	C2:86:4E:AB:23:06:A5:7B:2C:DA:90:F1:55:7E:AC:DB:88:B3:02:D8:EE:49:9A:5A:E9:38:EF:67:25:CB:E2:B1
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	C4:5D:7B:B0:8E:6D:67:E6:2E:42:35:11:0B:56:4E:5F:78:FD:92:EF:05:8C:84:0A:EA:4E:64:55:D7:58:5C:60
• 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	AA:2C:F1:40:B3:25:C5:78:D6:BA:61:15:FA:83:A3:38:AC:33:5E:27:45:3C:F7:A9:1A:63:5C:FE:D5:44:8D:4B
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	15:D5:B8:77:46:19:EA:7D:54:CE:1C:A6:D0:B0:C4:03:E0:37:A9:17:F1:31:E8:A0:4E:1E:6B:7A:71:BA:BC:E5
• 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	EB:73:A1:6A:1D:61:DD:86:18:68:78:EB:2B:C3:48:5D:1C:0C:A5:F0:4E:55:E4:FD:A1:37:85:CD:6C:8F:BC:B0
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	71:CC:A5:39:1F:9E:79:4B:04:80:25:30:B3:63:E1:21:DA:8A:30:43:BB:26:66:2F:EA:4D:CA:7F:C9:51:A4:BD
• 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	F5:AB:D3:F1:C6:66:7C:37:0E:24:D7:37:EF:89:1C:9D:64:CE:B6:6A:C0:DE:66:1D:42:5E:D3:65:BB:96:10:91

Root/Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
Google Trust Services - GlobalSign Root CA-R2	9B:E2:07:57:67:1C:1E:C0:6A:06:DE:59:B4:9A:2D:DF:DC:19:86:2E	04:00:00:00:00:01:0F:86:26:E6:0D	CA:42:DD:41:74:5F:D0:B8:1E:B9:02:36:2C:F9:D8:BF:71:9D:A1:BD:1B:1E:FC:94:6F:5B:4C:99:F4:2C:1B:9E
• 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	98:DA:04:2C:EB:04:BA:52:E9:E4:D7:C6:1E:43:BD:76:F9:4E:88:DC:FF:8E:F1:EF:73:52:0D:EB:6F:98:1B:82
• 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	BE:0C:CD:54:D4:CE:CD:A1:BD:5E:5D:9E:CC:85:A0:4C:2C:1F:93:A5:22:0D:77:FD:E8:8F:E9:AD:08:1F:64:1B
• 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	95:C0:74:E3:59:02:A1:4A:BD:9D:19:AF:B6:E7:F8:0E:66:9F:F8:E2:36:32:70:53:9D:96:36:13:F0:4A:AA:21
• 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	D5:70:84:C1:27:98:73:27:1E:B2:CE:7B:84:15:A4:1C:E9:12:6B:54:4D:85:18:BA:D8:7F:F1:CE:5A:60:4D:A3
Google Trust Services - GlobalSign ECC Root CA - R4	54:B0:7B:AD:45:B8:E2:40:7F:FB:0A:6E:FB:BE:33:C9:3C:A3:84:D5	2A:38:A4:1C:96:0A:04:DE:42:B2:28:A5:0B:E8:34:98:02	BE:C9:49:11:C2:95:56:76:DB:6C:0A:55:09:86:D7:6E:3B:A0:05:66:7C:44:2C:97:62:B4:FB:B7:73:DE:22:8C
• 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	61:72:77:3E:0B:60:BB:E7:48:D0:5E:75:B9:49:51:7E:30:66:8D:3F:6F:4B:9C:03:45:22:6F:67:F2:F7:5A:9C

Appendix B

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
1	GTS publicly disclosed a Signed Certificate Timestamps (SCT) issue on August 23, 2018. A coding error resulted in SCTs being logged to two Google Certificate Transparency (CT) logs instead of one Google CT and one non-Google CT log as required by the Chrome browser policy. The error resulted in warnings being displayed in Chrome Canary (v67) that had Certificate Transparency checks enabled. The issue was fully resolved within 14 hours after initial notification.	N/A – there was no impact on the WebTrust Principles and Criteria for Certification Authorities Version 2.1. GTS has shared the issue in the interest of transparency and knowledge sharing.	**Mozilla Dev Security Policy Link**