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 and Google Trust Services Europe Limited:

We have examined the accompanying assertion made by the management of Google Trust Services LLC and Google Trust Services Europe Limited (collectively, GTS), 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 Version 2.7* that for its Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma USA, Ghlin, Belgium, and Zurich, Switzerland for CAs as enumerated in **Appendix A,** throughout the period from October 1, 2022 through September 30, 2023. GTS has:

- Disclosed its SSL certificate lifecycle management business practices in its:
    - Google Trust Services, Certification Practices Statement v.4.21; and
    - Google Trust Services, TLS Certificate Policy v.3.7

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the GTS 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 GTS)
- 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 Version 2.7*.

GTS' management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the *WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7*.

Our responsibility is to express an opinion on GTS 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.

GTS' management has disclosed to us the attached matters referenced in **Appendix B** that the Company has 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 matters in our risk assessment and 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. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

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

We are required to be independent of GTS and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

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. Further, 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.

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 – SSL Baseline with Network Security Version 2.7*, or the suitability of any of GTS' services for any customer's intended purpose.

GTS' 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.

Ernst & Young LLP

October 31, 2023

1600 Amphitheatre Parkway
Mountain View, California 94043

Google Trust Services LLC

Tel: 650.253.0000
www.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 v2.7

We, as the management of Google Trust Services LLC and Google Trust Services Europe Limited (collectively, GTS), are responsible for operating the SSL Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich, Switzerland for the Root and Subordinate CAs 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 GTS' CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management of GTS 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 New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich Switzerland throughout the period from October 1, 2022, through September 30, 2023, GTS has:

- Disclosed its SSL certificate lifecycle management business practices in its:
    - Google Trust Services, Certification Practices Statement v.4.21; and
    - Google Trust Services, TLS Certificate Policy v.3.7

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the GTS 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 GTS)

- 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 Root and Subordinate CAs 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 Version 2.7*,

Very truly yours,

GOOGLE TRUST SERVICES LLC &

GOOGLE TRUST SERVICES EUROPE LIMITED

October 31, 2023

Appendix A:

Table 1: Root CAs

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=Google Trust Services - GlobalSign ECC Root CA - R4 O=GlobalSign C=Not applicable	54B07BAD45B8E2407FFB0A6EFBBE33C93CA384D5	0203E57EF53F93FDA50921B2A6	B085D70B964F191A73E4AF0D54AE7A0E07AAFDAF9B71DD0862138AB7325A24A2
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F52662CEFF08913713E	0203E5936F31B01349886BA217	D947432ABDE7B7FA90FC2E6B59101B1280E0E1C7E4E40FA3C6887FFF57A7F4CF
CN=GTS Root R1 Cross O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F52662CEFF08913713E	77BD0D6CDB36F91AEA210FC4F058D30D	3EE0278DF71FA3C125C4CD487F01D774694E6FC57E0CD94C24EFD769133918E5
CN=GTS Root R2 O=Google Trust Services LLC C=US	BBFFCA8E239F4F99CADBE268A6A51527171ED90E	0203E5AEC58D04251AAB1125AA	8D25CD97229DBF70356BDA4EB3CC734031E24CF00FAFCFD32DC76EB5841C7EA8
CN=GTS Root R3 O=Google Trust Services LLC C=US	C1F126BAA02DAE8581CFD3F12A12BDB80A67FDBC	0203E5B882EB20F825276D3D66	34D8A73EE208D9BCDB0D956520934B4E40E69482596E8B6F73C8426B010A6F48
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	0203E5C068EF631A9C72905052	349DFA4058C5E263123B398AE795573C4E1313C83FE68F93556CD5E8031B3C7D

Table 2: Subordinate CAs

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Additional Information
CN=GTS CA 2D5 O=Google Trust Services LLC C=US	1556BFF2453E18C48E15C60F3EC721284B0A857C	7F57F3C4CA39F4BEC6649F26E77E82D4	EDBCDD01698D83EAFA1E3D38F017B3AD96B2D8D88E746C58011CEE0EF106939C	
CN=GIAG4 ECC O=Google Trust Services LLC C=US	808CFC160AC8F399CE5C93BF63E34A96CB9C99B4	01F09C578AE0E9FC1855867C64	CAF3A229D454597F262939F07E105683A71FDCF91646FC60A32AF6B354FE52AE	Revoked on 13 June 2023
CN=GTS CA 2D4 O=Google Trust Services LLC C=US	A888D98A39AC65D5824B37A8956C6543CD4401E0	021668F1CD0A2A8F847D8AAD34	834B5BE6BD66A404F68F6EC9DE1C1E5C5723DDA65A7D3F66FB6209969D8854D8	Revoked on 18 September 2023
CN=GTS CA 1C3 O=Google Trust Services LLC C=US	8A747FAF85CDEE95CD3D9CD0E24614F371351D27	0203BC53596B34C718F5015066	23ECB03EEC17338C4E33A6B48A41DC3CDA12281BBC3FF813C0589D6CC2387522	
CN=GTS CA 1D4 O=Google Trust Services LLC C=US	25E2180EB25791942AE5D45D869083DE53B3B892	02008EB2023336658B64CDDB9B	64E286B76063602A372EFD60CDE8DB2656A49EE15E84254B3D6EB5FE38F4288B	
CN=GTS CA 1P5 O=Google Trust Services LLC C=US	D5FC9E0DDF1ECADD0897976E2BC55FC52BF5ECB8	0203BC50A32753F0918022EDF1	97D42003E132552946097F20EF955F5B1CD570AA4372D780033A65EFBE69758D	

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Additional Information
CN=GIAG4x O=Google Trust Services LLC C=US	EE0A93CED9D4F79AA99744503566D8CD7D6F5A10	0203F3588816160E0A4527F2A5	D3680B4E3F88DB1F5BB9DDDBFB6BFF319C780E3D9F44EE24EC1995AB42D6914F	Revoked on 13 June 2023
CN=GTS Y1 O=Google Trust Services LLC C=US	8622105D856025F23A1E7D0AAF612AB3151A0A77	01F0F79D5E7827FB40A912B310	7D740341B5193F53E675E3A1E3B4B1095E602509F65A5FA7576B0E3A5470F9C6	Revoked on 13 June 2023
CN=GTS CA 1D9 O=Google Trust Services LLC C=US	4AD0A481556E16D70B25785FAA9C3918053BA0AE	7F57F38B771162561FB3C18D61E5D8B9	02609E88979FC6862EA1571F3BC6DF6C70F2FE9277473E43FE04C3597C43431D	
CN=GTS Y2 O=Google Trust Services LLC C=US	6D65A2D7F3508F097865B162A2BE3CEDBB463A35	01F09C5B0EA22937CF9EE4416C	9C30516496E125B3D0931F49875E29516D9DC25473E5D6A106C1FCF866D306DB	Revoked on 13 June 2023
CN=GTS CA 1D8 O=Google Trust Services LLC C=US	90F850FAE79025C9E4277D12DD4758E7740FB66A	0219C15AC025A1B0A5C1D9D501	C0E8B1C195CDFF7B5137B9AD3513A6120B1DBFF49E5E0A8CEA3273BC8D761877	Revoked on 12 September 2023
CN=GTS CA 2D6 O=Google Trust Services LLC C=US	FAD34FA04DE872A65A16C12DF60A0EE46821AE7E	7F57F3D2EAF1C0CBA691B003C9FBD0A4	F5D12415A12C07FDE93BD6F9E4E4588E03D20596E4F8A5E9D213A83364BCEE71	

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Additional Information
CN=GTS Y3 O=Google Trust Services LLC C=US	AA63D582173D34533C45404C8C25DA87BCD19E1E	01FEA580C258A731CBC3B39EAB	181DC8BE7E91EDF163E66CC3FAD14D979A6DAE53B556DAEE8F7DCA0E114C14F6	Revoked on 13 June 2023
CN=GTS CA 2D3 O=Google Trust Services LLC C=US	BFA953BF1B69D88529349A6943CBD67AD499FF6D	021668D8D65BC4320E5B8E5E76	57BE32D0638809F1CB7C6B58D57CFFAEB99774B1F0B57D6A3708923954A54824	Revoked on 14 September 2023
CN=GTS CA 2A1 O=Google Trust Services LLC C=US	9318639117769A5AE63B7F2E338384866B1ED4F9	02008EB258E7B5940C1FF90044	11C697878732056DE17C1DA134E9D2B6D23CF1DE95B3FB0A4D18A517AB63230A	
CN=GTS CA 2P2 O=Google Trust Services LLC C=US	8723A950480E0789540A7130F633D20A47F69DAC	02166825E1700440612491F540	3647AAC2B282BC941FE7A642E3DCB99CFC5B3C6DCE944A1E96F8028E89B7B090	
CN=GTS Y4 O=Google Trust Services LLC C=US	B4A7998AF89149AC8E58B9B35E4FCC7098CD2267	01FEA581447E3BFD3BB81C2498	28676200C415D82D10251F527A773E7E7AC9902232FABA43E1A68C5AD3B7D87D	Revoked on 13 June 2023

Appendix B:

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
1	On 10/3/2022, GTS was notified that the CRL entry for one certificate contained a CRL reason code of 7, which is not a valid value of the *CRLReason* enumeration as defined in RFC 5280 section 5.3.1. GTS investigated this issue and determined that the incident was caused due to an incorrect mapping of *CRLReason* within their internal code base to the codes prescribed within RFC 5280 section 5.3.1. On further investigation, it was identified that a total of three certificates, revoked on 7/29/2022, were impacted. In response to this incident, GTS implemented a fix on 10/6/2022 to correct the affected reason codes. The incident was closed in Bugzilla on 10/26/2022, during the current examination period.	2.2.6 - The CA maintains controls to provide reasonable assurance that with exception to the requirements stipulated in the Baseline Requirements Sections 7.1.2.1, 7.1.2.2, and 7.1.2.3, all other fields and extensions of certificates generated after the Effective Date (1 July 2012) are set in accordance with RFC 5280.	Bugzilla Link
2	On 2/9/2023, GTS was notified that Signed Certificate Timestamps (SCT), which are pre-certificate extensions, were incorrectly embedded in a portion of SXG certificates. 2271 SXG certificates were issued during the period, out of which 883 were impacted. This issue was in violation of RFC 6962, which only permits CAs to place the SCT extension in a final certificate when it contains SCTs that were obtained from the precertification. Therefore, the 883 active SXG certificates were issued with incorrect extensions. GTS fixed the issue on 2/15/2023 and added certificate SCT verification checks to the issuance verification checks. A unit test has been added to further mitigate the risk of reoccurrence. The incident was closed in Bugzilla on 3/20/2023, during the current examination period.	2.2.5 - The CA maintains controls to provide reasonable assurance that the extensions, key sizes, and certificate policy identifiers (including Reserved Certificate Policy Identifiers) of Subscriber certificates generated conform to the Baseline Requirements.	Bugzilla Link

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
3	On 6/8/2023, GTS issued a public statement stating that GTS failed to respond to a Certificate Problem Report (CPR) which requested revocation of a certificate, within 24 hours. GTS investigated the issue and determined that revocation requests sent via the contact form on the website to report CPRs, was no longer passing new requests into pipeline for review. The issue began on 6/4/2023 and impacted four CPR form submissions, one of which was determined to be a valid submission. Per further investigation, it was determined that revocation was not needed since the certificate had been issued to the third-party service provider of the subscriber. As such, no mis-issuances occurred, despite the failure to respond to the valid form submission in 24 hours. In response, the dependent service that caused the issue was fixed on 6/9/2023. To prevent future issues, GTS removed one of the significant dependencies of the CPR revocation request process and added checks to ensure that CPRs are responded to within the required 24-hour time frame. Furthermore, CPR visibility among the team was increased via additional notification mechanisms to avoid bottlenecks and improve response times. The incident is still open on Bugzilla during the current examination period due to open community discussion requesting more specific information on how GTS is updating their CPR process.	2.5.1 - The CA maintains controls to provide reasonable assurance that a process is available 24x7 that the CA is able to accept and respond to revocation requests and related inquiries, and that the CA provides a process for Subscribers to request revocation of their own certificates. 2.5.2 - The CA maintains controls to provide reasonable assurance that it: • has the capability to accept and acknowledge Certificate Problem Reports on a 24x7 basis; • identifies high priority Certificate Problem Reports; • begin investigation of Certificate Problem Reports within 24 hours and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report: • decides whether revocation or other appropriate action is warranted; • if revocation is deemed the appropriate action, the elapsed time from receipt of the Certificate Problem Report or revocation request and revocation status information does not exceed the timelines in SSL Baseline Requirements 4.9.1.1; and • where appropriate, forwards such complaints to law enforcement.	Bugzilla Link
4	On 6/15/2023, GTS issued a public statement stating that revocation information from a Subordinate Certificate Authority (Sub CA) ceremony performed on 6/13/2023 00:00 UTC revoking six (6) Subordinate CA Certificates had not been published within 24 hours of the revocation	2.5.6 - The CA maintains controls to provide reasonable assurance that an online 24x7 Repository is provided that application	Bugzilla Link

	Disclosure	Relevant WebTrust Criteria	Publicly Disclosed Link
	ceremony. The CRL/OCSP responses were published on 6/15/2023 12:37 UTC, 48 hours after the revocation ceremony. In response to this incident, GTS implemented a linter, a UNIX software tool, for the ceremony tool input to identify if the revocation time does not allow sufficient time for the publishing and propagation of revocation data. In addition, a post-ceremony checklist, which includes deadlines for each post-ceremony activity, was added to GTS' ceremony document template. The incident was closed on Bugzilla on 7/28/2023, during the current examination period.	software can use to automatically check the current status of all unexpired Certificates issued by the CA, and: • for the status of subordinate CA Certificates - 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."	