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:

Scope
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 Certificate Authority Operations Based on the WebTrust Principles and Criteria for Certification Authorities – Network Security Version 1.7* 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 September 1, 2023 through August 31, 2024. GTS has:

- 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 – Network Security Version 1.7.*

Management's responsibilities
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 – Network Security v1.7*.

Our responsibilities
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.

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.

Building a better working world

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.

Other matters
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.

Inherent Limitations
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.

Opinion
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 – Network Security Version 1.7*, or/the suitability of any of GTS' services for any customer's intended purpose.

GTS' use of the WebTrust for Certification Authorities – 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 3, 2024

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 Certificate Authority Operations Based on the WebTrust Principles and Criteria for Certification Authorities Network Security v1.7

We, as the management of Google Trust Services LLC and Google Trust Services Europe Limited (collectively, GTS), are responsible for operating a Certification Authority (CA) at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich, Switzerland for the Root and Subordinate listed at **Appendix A**.

The management of GTS is responsible for establishing and maintaining effective controls over its CA services, including its network and certificate system security 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 its controls over its CA services. Based on that assessment, in providing its Certification Authority (CA) services at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich Switzerland throughout the period from September 1, 2023 through August 31, 2024, GTS has:

- 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 Network Security Requirements at **Appendix A**, based on the *WebTrust Principles and Criteria for Certification Authorities – Network Security Version 1.7*

Very truly yours,

GOOGLE TRUST SERVICES LLC &

GOOGLE TRUST SERVICES EUROPE LIMITED

October 3, 2024

Appendix A:

Table 1: Root CAs

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Applicable Notes
CN=GlobalSign OU=GlobalSign ECC Root CA - R4 O=GlobalSign	54B07BAD45B8E2407FFB0A6EFBBE33C93CA384D5	0203E57EF53F93FDA50921B2A6	B085D70B964F191A73E4AF0D54AE7A0E07AAFDAF9B71DD0862138AB7325A24A2	
CN=GlobalSign OU=GlobalSign ECC Root CA - R4 O=GlobalSign	54B07BAD45B8E2407FFB0A6EFBBE33C93CA384D5	2A38A41C960A04DE42B228A50BE8349802	BEC94911C2955676DB6C0A550986D76E3BA005667C442C9762B4FBB773DE228C	Historical Root CA Certificate
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F52662CEFF08913713E	0203E5936F31B01349886BA217	D947432ABDE7B7FA90FC2E6B59101B1280E0E1C7E4E40FA3C6887FFF57A7F4CF	
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F52662CEFF08913713E	6E47A9C54B470C0DEC33D089B91CF4E1	2A575471E31340BC21581CBD2CF13E158463203ECE94BCF9D3CC196BF09A5472	Historical Root CA Certificate
CN=GTS Root R2 O=Google Trust Services LLC C=US	BBFFCA8E239F4F99CADBE268A6A51527171ED90E	0203E5AEC58D04251AAB1125AA	8D25CD97229DBF70356BDA4EB3CC734031E24CF00FAFCFD32DC76EB5841C7EA8	
CN=GTS Root R2 O=Google Trust Services LLC C=US	BBFFCA8E239F4F99CADBE268A6A51527171ED90E	6E47A9C65AB3E720C5309A3F6852F26F	C45D7BB08E6D67E62E4235110B564E5F78FD92EF058C840AEA4E6455D7585C60	Historical Root CA Certificate
CN=GTS Root R3 O=Google Trust Services LLC C=US	C1F126BAA02DAE8581CFD3F12A12BDB80A67FDBC	0203E5B882EB20F825276D3D66	34D8A73EE208D9BCDB0D956520934B4E40E69482596E8B6F73C8426B010A6F48	

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Applicable Notes
CN=GTS Root R3 O=Google Trust Services LLC C=US	C1F126BAA02DAE8581CFD3F12A12BDB80A67FDBC	6E47A9C76CA9732440890F0355DD8D1D	15D5B8774619EA7D54CE1CA6D0B0C403E037A917F131E8A04E1E6B7A71BABCE5	Historical Root CA Certificate
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	0203E5C068EF631A9C72905052	349DFA4058C5E263123B398AE795573C4E1313C83FE68F93556CD5E8031B3C7D	
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	6E47A9C88B94B6E8BB3B2AD8A2B2C199	71CCA5391F9E794B04802530B363E121DA8A3043BB26662FEA4DCA7FC951A4BD	Historical Root CA Certificate

Table 2: Subordinate CAs

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=AE1 O=Google Trust Services C=US	488960F9A37D0CEA0024A2DC9F07CE4688A8323A	7FF4E5CE36A6A1FA5EE1916C08D39B7C	812C212E9E45DC5005C7F47411183F5FB2FF1BAEE184D3354B2E93D78C280164
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 1D9 O=Google Trust Services LLC C=US	4AD0A481556E16D70B25785FAA9C3918053BA0AE	7F57F38B771162561FB3C18D61E5D8B9	02609E88979FC6862EA1571F3BC6DF6C70F2FE9277473E43FE04C3597C43431D
CN=GTS CA 1P5 O=Google Trust Services LLC C=US	D5FC9E0DDF1ECADD0897976E2BC55FC52BF5ECB8	0203BC50A32753F0918022EDF1	97D42003E132552946097F20EF955F5B1CD570AA4372D780033A65EFBE69758D
CN=GTS CA 2A1 O=Google Trust Services LLC C=US	9318639117769A5AE63B7F2E338384866B1ED4F9	02008EB258E7B5940C1FF90044	11C697878732056DE17C1DA134E9D2B6D23CF1DE95B3FB0A4D18A517AB63230A
CN=GTS CA 2D5 O=Google Trust Services LLC C=US	1556BFF2453E18C48E15C60F3EC721284B0A857C	7F57F3C4CA39F4BEC6649F26E77E82D4	EDBCDD01698D83EAFA1E3D38F017B3AD96B2D8D88E746C58011CEE0EF106939C
CN=GTS CA 2D6 O=Google Trust Services LLC C=US	FAD34FA04DE872A65A16C12DF60A0EE46821AE7E	7F57F3D2EAF1C0CBA691B003C9FBD0A4	F5D12415A12C07FDE93BD6F9E4E4588E03D20596E4F8A5E9D213A83364BCEE71
CN=GTS CA 2P2 O=Google Trust Services LLC C=US	8723A950480E0789540A7130F633D20A47F69DAC	02166825E1700440612491F540	3647AAC2B282BC941FE7A642E3DCB99CFC5B3C6DCE944A1E96F8028E89B7B090

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F52662CEFF08913713E	77BD0D6CDB36F91AEA210FC4F058D30D	3EE0278DF71FA3C125C4CD487F01D774694E6FC57E0CD94C24EFD769133918E5
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FCB53EC56AF0941D8C	7FE530BF331343BEDD821610493D8A1B	76B27B80A58027DC3CF1DA68DAC17010ED93997D0B603E2FADBE85012493B5A7
CN=MR1 O=Google Trust Services C=US	9A541A6669C30CDA535C16536A13FE620E803FF1	7FF4E5CF7619B94F30F8A47FF8749148	BDF40C618E862D9B6B52718A1FB35BB951DFDBD2428B17D8A3FC64DF9E5DF355
CN=WE1 O=Google Trust Services C=US	9077923567C4FFA8CCA9E67BD980797BCC93F938	7FF31977972C224A76155D13B6D685E3	1DFC1605FBAD358D8BC844F76D15203FAC9CA5C1A79FD4857FFAF2864FBEBF96
CN=WE1 O=Google Trust Services C=US	9077923567C4FFA8CCA9E67BD980797BCC93F938	7FF357689BC24E302D90E18A41BD0E1F	A287FFAB762CC69A26D482037EDF701F653CE899025C62A7E5CB88BB9B419CBB
CN=WE2 O=Google Trust Services C=US	75BEC477AE89F644377DCFB1681F1D1AEBDC3459	7FF32D6B409D15D5965B05873A7C72E0	9C3F2FD11C57D7C649AD5A0932C0F0D29756F6A0A1C74C43E1E89A62D64CD320
CN=WE2 O=Google Trust Services C=US	75BEC477AE89F644377DCFB1681F1D1AEBDC3459	7FF3577FF63C7CA37E0642F8C8B86290	54F8CA858BCC7591F28D8DC3772E9BC581717F3A23A288BFD405939C36208DE5
CN=WE3 O=Google Trust Services C=US	36B62CCEA3B4D0409045F38B4581C1C8E319D46D	7FF32D6DBD5EDD54CA4E4B6795729143	9F819A4C876E12DC84E6FE0E37C1A69B137094B453FA98449398F4B71F4D0092
CN=WE3 O=Google Trust Services C=US	36B62CCEA3B4D0409045F38B4581C1C8E319D46D	7FF357910F07E1929F3D0084AEF198C7	54C660DA29D75FC81F07AD6DC8BB7AEE2258E071E8B1077544FA5622FF44C99D
CN=WE4 O=Google Trust Services C=US	6DE7D465B438575695CDE5B4775A360ADE7D52A6	7FF32D70BBD1A7309B5732500AC99AAE	D0C97E56C7B0BA812D944AD771F7799B5D4144A2327A4E416554F7EE2AA0AEAE

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=WE4 O=Google Trust Services C=US	6DE7D465B438575695CDE5B4775A360ADE7D52A6	7FF357A2DCFA8935B32362F61523B3A7	9D5E86906A1680A86BE278CF76E3D2B62B775186101461D303CEE910D94CE13A
CN=WE5 O=Google Trust Services C=US	D465CB38C7253C286BE97E43C3A1A1B8E44C68A0	7FF4E5CBECD981F2ADFA08913CEFAB14	847409E63526F162753AC49F75218EFAAFA7D5C94ADE9095CE72E7F6B6E3AC99
CN=WR1 O=Google Trust Services C=US	666949D4DE2A9C9103CF890E24B80E30036E882E	7FD9E2C2D2048A0474B627A26D0868A7	B10B6F00E609509E8700F6D34687A2BFCE38EA05A8FDF1CDC40C3A2A0D0D0E45
CN=WR2 O=Google Trust Services C=US	DE1B1EED7915D43E3724C321BBEC34396D42B230	7FF005A07C4CDED100AD9D66A5107B98	E6FE22BF45E4F0D3B85C59E02C0F495418E1EB8D3210F788D48CD5E1CB547CD4
CN=WR3 O=Google Trust Services C=US	C781F5FD8E88D9003C4D63A2503124A0CE23FE23	7FF005A91568D63ABC22861684AA4B5A	2FE357DB13751FF9160E87354975B3407498F41C9BD16A48657866E6E5A9B4C7
CN=WR4 O=Google Trust Services C=US	9BC811BC3DAA36B9318C4E8F44D557322FC3C061	7FF005B4DA75B86A5AC61FE4307713CD	DC9416C2F855126D6DE977677538F2F967FF4998E90DFA435A17219BE077FC06
CN=WR5 O=Google Trust Services C=US	4C5B19C28F1A7F556FAA1029FA028BC73C2A223C	7FF4E5C91496B0F2A18905ED501E62A3	AE0FC852280F1B87CEDAF73CFB84CF106EFEC88E8294253AF352ED4034460D7B

Appendix B:

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the Network Security criteria.*

	Disclosure	Relevant Network Security Criteria	Publicly Disclosed Link
1	On February 29, 2024, GTS issued a public statement stating GTS OCSP responders incorrectly responded to requests with an “unauthorized” status for certificates issued by two (2) new intermediate CAs (WE2 and WR2), which impacted 3,301 OCSP responses. GTS' legacy OCSP responder includes an additional pipeline to periodically push status information refreshes for each Sub CA before the status information is propagated. As such, the legacy OCSP responder depends upon the source pipeline to provide the correct information. GTS investigated the issue and determined that the OCSP responders relying on legacy OCSP pipeline were misconfigured for two (2) new intermediate CAs (WE2 and WR2), invalidating any updates received. Thus, the status information was lost, and the responders began returning an “unauthorized” response for the certificates issued under the two impacted CAs. In response to this incident, GTS implemented automation to generate OCSP information for new intermediate CAs, limiting the risk of manual human error, and to ensure their legacy OCSP pipeline is agnostic to intermediate CA addition and removal. GTS also introduced additional monitoring around OCSP and CRLs when a new intermediate CA is configured. The incident was closed in Bugzilla on May 5, 2024, during the current examination period.	**N/A**	Google Trust Services: Incorrect OCSP responses for new ICAs under test Incorrect (#1882904)

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the Network Security criteria.*

	Disclosure	Relevant Network Security Criteria	Publicly Disclosed Link
2	On January 25, 2024, GTS issued a public statement stating that the IP validation record for one (1) Alphabet owned IP address was not properly retained during the issuance process, impacting 58 certificates, 12 of which were active at the time of incident discovery. The incident was due to a manual error, as the CAE who approved issuance of the certificate did so without the submission of validation evidence. In response to the incident, GTS implemented technical controls to validate identifiers prior to adding them to validation flat files. The incident was closed in Bugzilla on April 17, 2024, during the current examination period.	**N/A**	Google Trust Services: Failure to properly validate IP address (#1876593)
3	On June 14, 2024, GTS issued a public statement stating that 58 SXG certificates were issued without the presence of "issue" or "issuewild" CAA property. 12 were active at the time the incident was discovered. The incident is limited to SXG-specific CAA validation requirements, and did not impact SSL certificates. All affected certificates complied to the SSL CAA checking requirements. The incident occurred as GTS failed to consider the corner cases where the required "issue" and "issuewild" properties were absent, but other properties were included, leading the CAA validation to succeed where it should have failed. Further, GTS revoked the impacted certificates within 24 hours of discovering the incident. In response to this incident, GTS implemented several new unit tests for SXG CAA, to catch such issues prior to deployment to production. Further, GTS added references within their code to clarify the CAA requirements for future developers and reviewers. The incident was closed in Bugzilla on July 31, 2024, during the current examination period.	**N/A**	Google Trust Services: SXG certificates issued without correctly checking CAA restrictions (#1902670)

**Note: GTS disclosed these incidents as included here for reference but there was no impact on the Network Security criteria.*

	Disclosure	Relevant Network Security Criteria	Publicly Disclosed Link
4	On June 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 June 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 June 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 was closed within the current examination period on November 2, 2024 due to open community discussion requesting more specific information on how GTS is updating their CPR process. This incident did not impact any CPRs during the current examination period.	**N/A**	Google Trust Services: Failure to respond to CPR within 24 hours (#1837519)