

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 Services Principles and Criteria for Certification Authorities Version 2.2.2* that for its Certification Authority (CA) operations at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich, Switzerland, for the Root and Subordinate CAs referenced in **Appendix A** and the key pairs that have been generated but are not in use as referenced in **Appendix C**, during the period from October 1, 2024 to September 30, 2025, GTS has:

- Disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in the applicable versions of its Certification Practice Statement (CPS) and Certificate Policies (CP) as referenced in **Appendix B**.
- Maintained effective controls to provide reasonable assurance that:
 - GTS' Certification Practice Statements are consistent with its Certificate Policies; and
 - GTS provides its services in accordance with its Certificate Policies and Certification Practice Statements
- Maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
 - the 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



Shape the future
with confidence

based on the [WebTrust Services Principles and Criteria for Certification Authorities Version 2.2.2.](#)

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 Services Principles and Criteria for Certification Authorities Version 2.2.2.*

GTS does not escrow its CA keys, does not provide subscriber key generation services, 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, does not provide external subordinate CA certificate services, and does not issue Extended Validation (EV) certificates. Further, GTS does not support certificate renewal or suspension. Accordingly, our examination did not extend to controls that would address those criteria.

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 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. 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's management has disclosed to us matters referenced in **Appendix D** 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. 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' 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.



Shape the future
with confidence

This report does not include any representation as to the quality of GTS' CA services beyond those covered by the *WebTrust Services Principles and Criteria for Certification Authorities Version 2.2.2* criteria, or the suitability of any of GTS' services for any customer's intended purpose.

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 to the future of any evaluations of effectiveness of specific controls is subject to the risk that controls may become ineffective.

Opinion

In our opinion, GTS' management's assertion referred to above, is fairly stated, in all material respects, based on the aforementioned criteria.

Use of the WebTrust Seal

GTS' use of the WebTrust for Certification Authorities 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 30, 2025



Google Trust Services LLC

Management's Assertion Regarding the Effectiveness of Its Controls Over the Certificate Authority Operations Based on the WebTrust Services Principles and Criteria for Certification Authorities Version 2.2.2

October 30, 2025

We, as 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 CAs and Subordinate CAs listed in **Appendix A** and the key pairs that have been generated but are not in use as referenced in **Appendix C**.

GTS' CA services provide the following certification authority services:

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

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.

There are inherent limitations in any controls, 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 services. Based on that assessment, in GTS Management's opinion, in providing its CA services for the Root CA(s) and Subordinate CA(s) listed in **Appendix A** at New York, USA, South Carolina, USA, Oklahoma, USA, Ghlin, Belgium, and Zurich, Switzerland and the private key pairs that have been generated but are not in use as referenced in **Appendix C** during the period from October 1, 2024 to September 30, 2025, GTS has:

- Disclosed its business, key lifecycle management, certificate life cycle management, and CA environmental control practices in the applicable versions of its Certification Practice Statement (CPS) and Certificate Policy (CP) as referenced in **Appendix B**



Google Trust Services LLC

- Maintained effective controls to provide reasonable assurance that:
 - GTS' Certification Practice Statements are consistent with its Certificate Policies; and
 - GTS provides its services in accordance with its Certificate Policies and Certification Practice Statements
- 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 were 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

based on the [WebTrust Services Principles and Criteria for Certification Authorities Version 2.2.2](#) including the following:

CA Business Practices Disclosure

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

CA Business Practices Management

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

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management



Google Trust Services LLC

- System Development, Maintenance, and Change Management
- Disaster Recovery, Backups, and 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
- CA Key Transportation
- CA Key Migration

Certificate Lifecycle Management Controls

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

Very truly yours,

GOOGLE TRUST SERVICES LLC &

GOOGLE TRUST SERVICES EUROPE LIMITED

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	54B07BAD45B8E2407FFB0A6EF BBE33C93CA384D5	0203E57EF53F93FDA 50921B2A6	B085D70B964F191A73E4AF0D54AE7A0E07 AAFDAF9B71DD0862138AB7325A24A2	
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F5266 2CEFF08913713E	0203E5936F31B01349 886BA217	D947432ABDE7B7FA90FC2E6B59101B1280 E0E1C7E4E40FA3C6887FFF57A7F4CF	
CN=GTS Root R2 O=Google Trust Services LLC C=US	BBFFCA8E239F4F99CADBE268 A6A51527171ED90E	0203E5AEC58D04251 AAB1125AA	8D25CD97229DBF70356BDA4EB3CC734031 E24CF00FAFCFD32DC76EB5841C7EA8	
CN=GTS Root R3 O=Google Trust Services LLC C=US	C1F126BAA02DAE8581CFD3F1 2A12BDB80A67FDBC	0203E5B882EB20F825 276D3D66	34D8A73EE208D9BCDB0D956520934B4E40 E69482596E8B6F73C8426B010A6F48	
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FC B53EC56AF0941D8C	0203E5C068EF631A9 C72905052	349DFA4058C5E263123B398AE795573C4E1 313C83FE68F93556CD5E8031B3C7D	
CN=GlobalSign OU=GlobalSign ECC Root CA - R4 O=GlobalSign	54B07BAD45B8E2407FFB0A6EF BBE33C93CA384D5	2A38A41C960A04DE4 2B228A50BE8349802	BEC94911C2955676DB6C0A550986D76E3B A005667C442C9762B4FBB773DE228C	Historical Root CA Certificate
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711A2B4827852F5266 2CEFF08913713E	6E47A9C54B470C0DE C33D089B91CF4E1	2A575471E31340BC21581CBD2CF13E15846 3203ECE94BCF9D3CC196BF09A5472	Historical Root CA Certificate
CN=GTS Root R2 O=Google Trust Services LLC C=US	BBFFCA8E239F4F99CADBE268 A6A51527171ED90E	6E47A9C65AB3E720C 5309A3F6852F26F	C45D7BB08E6D67E62E4235110B564E5F78F D92EF058C840AEA4E6455D7585C60	Historical Root CA Certificate

Root Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint	Applicable Notes
CN=GTS Root R3 O=Google Trust Services LLC C=US	C1F126BAA02DAE8581CFD3F1 2A12BDB80A67FDBC	6E47A9C76CA973244 0890F0355DD8D1D	15D5B8774619EA7D54CE1CA6D0B0C403E0 37A917F131E8A04E1E6B7A71BABCE5	Historical Root CA Certificate
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74FF4936A3D5D8FC B53EC56AF0941D8C	6E47A9C88B94B6E8B B3B2AD8A2B2C199	71CCA5391F9E794B04802530B363E121DA8 A3043BB26662FEA4DCA7FC951A4BD	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	488960F9A37 D0CEA0024A2 DC9F07CE468 8A8323A	7FF4E5CE36A6 A1FA5EE1916C0 8D39B7C	812C212E9E45DC5005C7F47411183F5FB2FF1BAEE184D3354B2E93D78C280164
CN=GTS Root R1 O=Google Trust Services LLC C=US	E4AF2B26711 A2B4827852F5 2662CEFF089 13713E	77BD0D6CDB36 F91AEA210FC4F 058D30D	3EE0278DF71FA3C125C4CD487F01D774694E6FC57E0CD94C24EFD769133918E5
CN=GTS Root R4 O=Google Trust Services LLC C=US	804CD6EB74F F4936A3D5D8 FCB53EC56AF 0941D8C	7FE530BF33134 3BEDD82161049 3D8A1B	76B27B80A58027DC3CF1DA68DAC17010ED93997D0B603E2FADBE85012493B5A7
CN=MR1 O=Google Trust Services C=US	9A541A6669C 30CDA535C16 536A13FE620 E803FF1	7FF4E5CF7619B 94F30F8A47FF8 749148	BDF40C618E862D9B6B52718A1FB35BB951DFDBD2428B17D8A3FC64DF9E5DF355
CN=WE1 O=Google Trust Services C=US	9077923567C4 FFA8CCA9E67 BD980797BCC 93F938	7FF31977972C2 24A76155D13B6 D685E3	1DFC1605FBAD358D8BC844F76D15203FAC9CA5C1A79FD4857FFAF2864FBEBF96
CN=WE1 O=Google Trust Services C=US	9077923567C4 FFA8CCA9E67 BD980797BCC 93F938	7FF357689BC24 E302D90E18A41 BD0E1F	A287FFAB762CC69A26D482037EDF701F653CE899025C62A7E5CB88BB9B419CBB
CN=WE2 O=Google Trust Services C=US	75BEC477AE8 9F644377DCF B1681F1D1AE BDC3459	7FF32D6B409D1 5D5965B05873A 7C72E0	9C3F2FD11C57D7C649AD5A0932C0F0D29756F6A0A1C74C43E1E89A62D64CD320

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=WE2 O=Google Trust Services C=US	75BEC477AE8 9F644377DCF B1681F1D1AE BDC3459	7FF3577FF63C7 CA37E0642F8C8 B86290	54F8CA858BCC7591F28D8DC3772E9BC581717F3A23A288BFD405939C36208DE5
CN=WE3 O=Google Trust Services C=US	36B62CCEA3B 4D0409045F38 B4581C1C8E3 19D46D	7FF32D6DBD5E DD54CA4E4B67 95729143	9F819A4C876E12DC84E6FE0E37C1A69B137094B453FA98449398F4B71F4D0092
CN=WE3 O=Google Trust Services C=US	36B62CCEA3B 4D0409045F38 B4581C1C8E3 19D46D	7FF357910F07E 1929F3D0084AE F198C7	54C660DA29D75FC81F07AD6DC8BB7AEE2258E071E8B1077544FA5622FF44C99D
CN=WE4 O=Google Trust Services C=US	6DE7D465B43 8575695CDE5 B4775A360AD E7D52A6	7FF32D70BBD1 A7309B5732500 AC99AAE	D0C97E56C7B0BA812D944AD771F7799B5D4144A2327A4E416554F7EE2AA0AEAE
CN=WE4 O=Google Trust Services C=US	6DE7D465B43 8575695CDE5 B4775A360AD E7D52A6	7FF357A2DCFA 8935B32362F61 523B3A7	9D5E86906A1680A86BE278CF76E3D2B62B775186101461D303CEE910D94CE13A
CN=WE5 O=Google Trust Services C=US	D465CB38C72 53C286BE97E 43C3A1A1B8E 44C68A0	7FF4E5CBECD9 81F2ADFA08913 CEFAB14	847409E63526F162753AC49F75218EFAAFA7D5C94ADE9095CE72E7F6B6E3AC99
CN=WR1 O=Google Trust Services C=US	666949D4DE2 A9C9103CF89 0E24B80E300 36E882E	7FD9E2C2D2048 A0474B627A26D 0868A7	B10B6F00E609509E8700F6D34687A2BFCE38EA05A8FDF1CDC40C3A2A0D0D0E45

Subordinate Name	Subject Key Identifier	Certificate Serial Number	SHA256 Fingerprint
CN=WR2 O=Google Trust Services C=US	DE1B1EED791 5D43E3724C3 21BBEC34396 D42B230	7FF005A07C4C DED100AD9D66 A5107B98	E6FE22BF45E4F0D3B85C59E02C0F495418E1EB8D3210F788D48CD5E1CB547CD4
CN=WR3 O=Google Trust Services C=US	C781F5FD8E8 8D9003C4D63 A2503124A0C E23FE23	7FF005A91568D 63ABC22861684 AA4B5A	2FE357DB13751FF9160E87354975B3407498F41C9BD16A48657866E6E5A9B4C7
CN=WR4 O=Google Trust Services C=US	9BC811BC3DA A36B9318C4E 8F44D557322F C3C061	7FF005B4DA75B 86A5AC61FE430 7713CD	DC9416C2F855126D6DE977677538F2F967FF4998E90DFA435A17219BE077FC06
CN=WR5 O=Google Trust Services C=US	4C5B19C28F1 A7F556FAA10 29FA028BC73 C2A223C	7FF4E5C91496B 0F2A18905ED50 1E62A3	AE0FC852280F1B87CEDAF73CFB84CF106EFEC88E8294253AF352ED4034460D7B

Appendix B

Google Trust Services, S/MIME Certificate Policy/Certification Practice Statement

Version Number	Effective Date
6.2	September 18, 2025
6.1	August 4, 2025
6.0	July 22, 2025

Google Trust Services, TLS Certificate Policy/Certification Practice Statement

Version Number	Effective Date
6.0	July 22, 2025

Google Trust Services Certification Practice Statement

Version Number	Effective Date
5.22	June 25, 2025
5.21	April 28, 2025
5.20	April 4, 2025
5.19	February 19, 2025
5.18	January 13, 2025
5.17	January 10, 2025
5.16	January 8, 2025
5.15	December 10, 2024
5.14	November 24, 2024
5.13	November 20, 2024
5.12	November 15, 2024

Google Trust Services TLS Certificate Policy

Version Number	Effective Date
4.11	January 9, 2025
4.10	December 10, 2024
4.9	November 27, 2024
4.8	November 20, 2024
4.7	November 15, 2024

Google Trust Services S/MIME Certificate Policy

Version Number	Effective Date
2.8	January 13, 2025
2.7	January 10, 2025

Appendix C:

Table 1: RSA Keys

Key Name	Subject Key Identifier
RSA Key #7	6fca05ca4afb2e093015580f850d803de891f58a
RSA Key #8	3d035448767062b005e8956d339ccbe303eb5b52
RSA Key #9	b26440d8c508bf4c7d58fa96edd22d35eb26788b
RSA Key #10	8f0a82e0e52bf8167d6d1ad852ae334885b558b2
RSA Key #11	e1ab26b08a8f6a5fa8d239cdcbdd0fff6609f693
RSA Key #12	a9477cb7a5a3b0c9c4d96bc2b8fa95257558e1b7
RSA Key #13	3901c12340be2784c73a32e2d3cf0ac4d7d64d24
RSA Key #14	0f382f3b9374d95f5162bc491b50fb8e21ab7a52
RSA Key #15	5e187cb280268a0a3b67268fa7c8c5c7c06569f2
RSA Key #16	f6d56e85fca89f8d95e7971a389817d95fa3c2d3
RSA Key #17	ca83444a5077b7d99197ad88445a14dd6c49279a
RSA Key #18	b3cf9d8f56a9c393859f371cc887a0a938efbb5f
RSA Key #19	22bce43c18f38acc5f1b779fb2ce4c951555e175
RSA Key #20	a2f6077fb99f120e04233a8c84a8ecbf93355e9b
RSA Key #21	6fb2612be3f628b85274daa8b1213836f8287a8e

Table 2: ECC Keys

Key Name	Subject Key Identifier
ECC Key #7	6fbaccb3d4ea6ce6c176ba2c1042691d2f99e793
ECC Key #8	f61b1c8a68cc74b76f585c02937312ad6bf38e2
ECC Key #9	211715fa0cce1793e7eb57860510600122954f5a
ECC Key #10	3906a53d2cacd8edbfd13e0a9a3c87398ad1f97c
ECC Key #11	3938cd386208e5d53b304e9dc68f4a4d14e25d84
ECC Key #12	d18022995b8289b04e16d5976b30ed0bc576275e
ECC Key #13	f529e87ed03a1657d95eaa713e0154a8bd843005
ECC Key #14	3220db7db178df27fcac3370d365c0a592f8dda8
ECC Key #15	f22900eb0a1194bb983541826b94ba9675459fec
ECC Key #16	d3feb3f47dd96989ac60e622be728e1c7a32b6fa
ECC Key #17	4bbc18107a4447535ded578cd30a8f884e83addd
ECC Key #18	2dec765e08b50e39752e4231f4c5472b1cb7c452
ECC Key #19	3559fcd26d3f1f7bc495ee37428dab230dc3e1af
ECC Key #20	cedf234b87ba4a53d870395091b59fe0687f3f12
ECC Key #21	4e2e26941352bb48367f52c76db740aefdec0b45
ECC Key #22	8eddb4d32b615d693aa825732e1566962e95b69b
ECC Key #23	a9e441da43a6e7619b291c2a53aff78f1032bd97
ECC Key #24	9600d52c8e4eb7548652a976354dd34aa5a6d265
ECC Key #25	ca131278df73f73ec5c62337c9170517e12efa49
ECC Key #26	799535533e4cb0858e282e6a51a75242d81be460
ECC Key #27	d32db941215439af6b78719f3be1e2e8d747cc9b
ECC Key #28	61f4a30e2f787cd2ab8fca638223dea0fe591da0
ECC Key #29	096b5c2da71d464db11ef3a3ff1cda8812919c81
ECC Key #30	5cac705f17a35f0ce4e4aaed06ffe8bc48c9bb88
ECC Key #31	943b639c12a1f39ecb984cffa5cfa94e81c2bff
ECC Key #32	bd058282185a9bd988d7da552c6edb960e5978d2

Appendix D:

	Disclosure	Publicly Disclosed Link
1	<p>On November 14, 2024, GTS issued a public statement stating that during the onboarding process for one (1) new hire, it was identified that membership to some access groups was granted in a different order than their procedures specified.</p> <p>In this case, training was complete, but the examination had not been completed before membership to access control groups was granted. The incident was due to the complexity and sequencing of the onboarding process.</p> <p>In response to this incident, GTS implemented changes to revise the access grant process to ensure that access is granted only after the new hire passes the onboarding examination. In addition, GTS reduced and simplified the sequencing of steps/approvals for onboarding new team members.</p> <p>The incident was closed in Bugzilla on December 27, 2024, during the current examination period.</p>	<p>Google Trust Services: New hire onboarding deviation from written procedure (#1931413)</p>
2	<p>On February 14, 2025, GTS issued a public statement stating that a bug in GTS' self-auditing tool resulted in the incorrect verification of the Multi-Perspective Issuance Corroboration (MPIC) perspectives used in domain control validation.</p> <p>The bug occurred due to GTS updating the format of the audit logs without also simultaneously updating the audit tool logic.</p> <p>In response to the incident, GTS fixed the bug and made improvements to its data gathering tools to improve the speed of analysis for future incident responses.</p> <p>The incident was closed in Bugzilla on March 14, 2025, during the current examination period.</p>	<p>Google Trust Services: Self-audit tooling MPIC perspective verification inconsistency (#1948368)</p>
3	<p>On April 10, 2025, GTS issued a public statement stating that 528,586 certificates lacked the desired number of remote perspective details for CAA checks.</p> <p>The incident occurred as issuance flow sometimes continued even when not all remote perspective CAA checks had completed and there was insufficient review of dark launch validation results and incorrect logging levels.</p> <p>In response to this incident, GTS halted issuance and fixed the initial issue as soon as the problem was confirmed. Further, GTS added test coverage to ensure the previous behavior could not recur and dashboards were updated to have finer grained metrics.</p> <p>The incident was closed in Bugzilla on June 10, 2025, during the current examination period.</p>	<p>Google Trust Services: Inconsistent MPCA secondary perspective logging (#1959867)</p>

	Disclosure	Publicly Disclosed Link
4	<p>On July 25, 2025, GTS issued a public statement stating that one (1) certificate was issued without one of its certificate lifecycle events being recorded in the audit log.</p> <p>The root cause of the incident was that an authorization database record was created to indicate it was possible to issue a certificate, but the corresponding audit log entry was not written due to a race condition.</p> <p>In response to this incident, GTS implemented mitigations to prevent recurrence of the issue, including:</p> <ul style="list-style-type: none"> - Updating the CA software to not permit issuance until the authorization record exists in the database - Ensuring services respect lame-duck mode (i.e. Option for server to stop accepting new connections but complete in-flight work); and - Ensuring that resolver authentication credentials do not expire before being refreshed <p>Further, GTS noted an action item to perform a focused review of its code to identify and remediate other instances that could fail to write a log before issuing a certificate.</p> <p>The incident was closed in Bugzilla on October 22, 2025, which is outside of the current examination period.</p>	<p>Google Trust Services: Missing authorization audit log entry for certificate issuance (#1979457)</p>