Introduction:
1) Name of the CA Organization: Google Trust Services LLC (GTS)
2) CAs in Scope: This assessment applied to all CAs of GTS maintained in CCADB as per 20 November 2017.
3) Version of the BR used: GTS uses CA-Browser Forum BR 1.5.1
4) Document version used: GTS CPS 2.0 available at https://pki.goog/GTS-CPS-2.0.pdf (CPS)
5) Responses describe the CA's practices as of 20 November 2017. There are no responses which include an implementation plan.

BR Section Number	List the specific documents and section numbers of those documents which meet the requirements of each BR section	Explain how the CA's listed documents meet the requirements of each BR section.
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	Appendix D of the CPS	Provides document history with previous revisions of the CPS.
1.2.2. Relevant Dates Note the Compliance date for eachitem in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.	1.2.2	The CPS is up to date and the stated practices are fully implemented.
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.	1.3.2	The CPS states that GTS does not delegate RA responsibilities.
2.1. Repositories Provide the direct URLs to the CA's repositories	2.1	The link to the GTS repository is stated in that section. It is https://pki.goog

2.2. Publication of information "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> Copy the specific text that is used into the explanation in this row. (in English)	2.1	In Section 2.1 of the CPS GTS states the following: "Google represents that it will adhere to the latest version of the CP published in the Repository" The CP is a reinstatement of the Baseline Requirements.
2.2. Publication of information "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.	Links to the test pages are published in the Repository.	https://good.r1demo.pki.goog/ https://revoked.r1demo.pki.goog/ https://expired.r1demo.pki.goog/ https://good.r2demo.pki.goog/ https://revoked.r2demo.pki.goog/ https://expired.r2demo.pki.goog/ https://good.r3demo.pki.goog/ https://revoked.r3demo.pki.goog/ https://expired.r3demo.pki.goog/ https://good.r4demo.pki.goog/ https://revoked.r4demo.pki.goog/ https://expired.r4demo.pki.goog/ https://good.gsr2demo.pki.goog/ https://revoked.gsr2demo.pki.goog/ https://expired.gsr2demo.pki.goog/ https://good.gsr4demo.pki.goog/♀ https://revoked.gsr4demo.pki.goog/ https://expired.gsr4demo.pki.goog/
2.3. Time or frequency of publication Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.	2.3	"Google reviews and updates this CPS annually and publishes the updated version typically within seven (7) days after its approval."
2.4. Access controls on repositories Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.	2.4	The CPS states that the Repository is publicly available.

3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, indicate how your CP/CPS meets the requirements in this section of the BRs.	3.2.2	The certificate validation methods used by GTS are described in Section 3.2.2 CPS.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, indicate how your CP/CPS meets the requirements in this section of the BRs.	3.2.2	The certificate validation methods used by GTS are described in Section 3.2.2 CPS.
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, indicate how your CP/CPS meets the requirements in this section of the BRs.	3.2.2	The certificate validation methods used by GTS are described in Section 3.2.2 CPS.
3.2.2.4 Validation of Domain Authorization or Control Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS. The CA's CP/CPS must clearly describe the acceptable methods of domain validation. It is *not* sufficient for the CP/CPS to merely reference the BRs. Enough information must be directly provided in the CP/CPS for the reader to be able to understand how the CA performs domain validation.	3.2.2	The certificate validation methods used by GTS are described in Section 3.2.2 CPS.
3.2.2.4.1 Validating the Applicant as a Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.3 Phone Contact with Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.

3.2.2.4.5 Domain Authorization Document If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	3.2.2	Domain Authorization Documents are not normally used by GTS. They may be used as an alternative method of proving authorization if no other method of proof is available. The usage of a Domain Authorization Document would be handled on a case by case basis in accordance with Section 3.2.2.4.5 BR.
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	Not currently used by GTS.
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.8 IP Address If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.9 Test Certificate If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	No stipulation in this BR Section.
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.	N/A	Not currently used by GTS.
3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, indicate how your CA meets the requirements in this section of the BRs.	3.2.2	GTS obtains documentation of IP address assignment from the Internet Assigned Numbers Authority or performs a reverse-IP address lookup and then verifies control over the resulting Domain Name under Section 3.2.2.4. BR.
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then indicate how your CA meets the requirements in this seciton of the BRs.	3.2.2.6	Prohibited issuance of wildcard certificates is prevented by the tooling used for certificate issuance.

3.2.2.7 Data Source Accuracy Indicate how your CA meets the requirements in this section of the BRs.	3.2.2.7	The issuance procedure defines which data sources are considered Reliable Data Sources. It also requires the CA staff to verify that records are still valid before relying on them.
3.2.3. Authentication of Individual Identity	N/A	GTS does not issue OV certificates to natural persons.
3.2.5. Validation of Authority	3.2.5	
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.	1.3.1	All cross-certifications are listed in Section 1.3.1
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	4.1.1	
4.1.2. Enrollment Process and Responsibilities	4.1.2	
4.2. Certificate application processing	4.2	
4.2.1. Performing Identification and Authentication Functions Indicate how your CA identifies high risk certificate requests.	4.2.1	Google's issuance practice is currently limited to Google affiliate companies. This limits the risk associated with high risk certificate requests.
4.2.2. Approval or Rejection of Certificate Applications	4.2.2	
4.3.1. CA Actions during Certificate Issuance	4.3.1	
4.9.1.1 Reasons for Revoking a Subscriber Certificate Reasons for revoking certificates must be listed in the CA's CP/CPS.	4.9.1.1	The reasons are listed in Section 4.9.1.1 CPS
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate	4.9.1.2	
4.9.2. Who Can Request Revocation	4.9.2	
4.9.3. Procedure for Revocation Request	4.9.3	
4.9.5. Time within which CA Must Process the Revocation Request	4.9.5	
4.9.7. CRL Issuance Frequency	4.9.7	
4.9.9. On-line Revocation/Status Checking Availability	4.9.9.	
4.9.10. On-line Revocation Checking Requirements Indicate how your CA meets all of the requirements listed in this section, including support of GET, update frequency, preventing errounious return of "good" status.	4.9.10	

4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	4.9.11	
4.10.1. Operational Characteristics	4.10.1	
4.10.2. Service Availability	4.10.2	
5. MANAGEMENT, OPERATIONAL, and Physical CONTROLS	5	
5.2.2. Number of Individuals Required per Task	5.2.2.	
5.3.1. Qualifications, Experience, and Clearance Requirements	5.3.1	
5.3.3. Training Requirements and Procedures	5.3.3	
5.3.4. Retraining Frequency and Requirements	5.3.4	
5.3.7. Independent Contractor Controls	5.3.7	
5.4.1. Types of Events Recorded	5.4.1	
5.4.3. Retention Period for Audit Logs	5.4.3	
5.4.8. Vulnerability Assessments	5.4.8	
5.5.2. Retention Period for Archive	5.5.2	
5.7.1. Incident and Compromise Handling Procedures	5.7.1.	
6.1.1. Key Pair Generation	6.1.1.	
6.1.2. Private Key Delivery to Subscriber	6.1.2.	
6.1.5. Key Sizes	6.1.5	
6.1.6. Public Key Parameters Generation and Quality Checking	6.1.6	
6.1.7. Key Usage Purposes	6.1.7	
6.2. Private Key Protection and Cryptographic Module Engineering Controls	6.2	
6.2.5. Private Key Archival	6.2.5	
6.2.6. Private Key Transfer into or from a Cryptographic Module	6.2.6	
6.2.7. Private Key Storage on Cryptographic Module	6.2.7	
6.3.2. Certificate Operational Periods and Key Pair Usage Periods	6.3.2	
6.5.1. Specific Computer Security Technical Requirements	6.5.1	
7.1. Certificate profile	7.1	

7.1.1. Version Number(s)	7.1.1	
7.1.2. Certificate Content and Extensions; Application of RFC 5280	7.1.2	
7.1.2.1 Root CA Certificate	7.1.2.1	
7.1.2.2 Subordinate CA Certificate	7.1.2.2	
7.1.2.3 Subscriber Certificate	7.1.2.3	
7.1.2.4 All Certificates	7.1.2.4	
7.1.2.5 Application of RFC 5280	7.1.2.5	
7.1.3. Algorithm Object Identifiers	7.1.3	
7.1.4. Name Forms	7.1.4	
7.1.4.1 Issuer Information	7.1.4.1	
7.1.4.2 Subject Information	7.1.4.2	
7.1.4.3 Subject Information - Subordinate CA Certificates	7.1.4.3	
7.1.5. Name Constraints	7.1.5.	
7.1.6. Certificate Policy Object Identifier	7.1.6.	
7.1.6.1 Reserved Certificate Policy Identifiers	7.1.6.1	
7.1.6.2 Root CA Certificates	7.1.6.2	
7.1.6.3 Subordinate CA Certificates	7.1.6.3	
7.1.6.4 Subscriber Certificates	7.1.6.4	
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	8	
8.1. Frequency or circumstances of assessment	8.1.	
8.2. Identity/qualifications of assessor	8.2	
8.4. Topics covered by assessment	8.4	
8.6. Communication of results	8.6	

Also indicate your understanding and compliance with Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers). "	N/A	We understand the cited requirements and belive that our audit reports in CCADB satisfy them with the exception of the SHA256 fingerprints. We will ask our auditors to include them in all subsequent reports they issue to us. (See comments in CCADB).
8.7. Self-Audits	8.7	
9.6.1. CA Representations and Warranties	9.6.1	
9.6.3. Subscriber Representations and Warranties	9.6.3	
9.8. Limitations of liability	9.8	
9.9.1. Indemnification by CAs	9.9.1	
9.16.3. Severability	9.16.3	

GTS CA Hierarchy						
Root CAs	**GTS Root R1**	**GTS Root R2**	**GTS Root R3**	**GTS Root R4**	**GS Root R2**	**GS Root R4**
Subordinate CAs	GTSX1	GTSX2	GTSX3	GTSX4	GIAG3	GIAG3 ECC
					GTS GIAG3	
					GTS CA 1O1	
					GTS CA 1D2	
					G2R2 (Operated by GlobalSign)	