Google Trust Services
Certification Practice Statement
v4.0

Contents

1. INTRODUCTION

1.1. Overview

The Google Public Key Infrastructure ("Google PKI"), has been established by Google Trust Services LLC ("Google"), to enable reliable and secure identity authentication, and to facilitate the preservation of confidentiality and integrity of data in electronic transactions. This document is issued by Google to identify the practices and procedures that Google employs in issuing certificates from its Certificate Authorities within the Google PKI.

1.2. Document name and identification

This document is the Google Certification Practice Statement (CPS). It has been published to describe procedural and operational practices that Google has adopted to implement the Google Certificate Policy (CP) and applicable requirements defined in governing industry standards.

The described practices relate to services and solutions used throughout the lifecycle of the CAs governed by this CPS and the certificates issued from them.

Google requires its affiliated entities, Applicants, Subscribers, and Relying Parties to who are involved in issuing and managing digital certificates within the Google PKI hierarchy to adhere to this CPS. Other important documents that accompany this CPS include the CP and associated Subscriber and Relying Party Agreements.

This CPS is structured in accordance with the Internet Engineering Task Force (IETF) standard RFC 3647.

1.2.1. Revisions

See Appendix D.

1.2.2. Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
2017-09-08	3.2.2.8	CAs MUST check and process CAA records
2018-08-01	3.2.2.4	The validation method in Section 3.2.2.4.1 BR may no longer be used
2018-10-14	4.9.1	Revocation timelines extended
2019-01-15	7.1.4.2.1	All certificates containing an underscore character in any dNSName entry and having a validity period of more than 30 days MUST be revoked prior to January 15, 2019
2019-05-01	7.1.4.2.1	underscore characters ("_") MUST NOT be present in dNSName entries
2019-08-01	3.2.2.5	IP Address validation methods updated
2020-06-03	3.2.2.4.6	CAs may not perform certificate validations using method 3.2.2.4.6

1.3. PKI participants

1.3.1. Certification authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue, manage, revoke, and renew certificates. Moreover it can refer to the infrastructure and key material from which such an entity issues and signs certificates.

This CPS covers all certificates issued and signed by the following CAs hereinafter referred to as 'Google CAs'.

Root CAs

- GTS Root R1
  Key: RSA 4096
  Serial#: 6e:47:a9:c5:4b:47:0c:0d:ec:33:d0:89:b9:1c:f4:e1
  Thumbprint: e1:c9:50:e6:ef:22:f8:4c:56:45:72:8b:92:20:60:d7:d5:a7:a3:e8
  Valid until: Jun 22, 2036

- GTS Root R1
  Key: RSA 4096
  Serial#: 02:03:e5:93:6f:31:b0:13:49:88:6b:a2:17
  Thumbprint: E5:8C:1C:C4:91:3B:38:63:4B:E9:10:6E:E3:AD:8E:6B:9D:D9:81:4A
  Valid until: Jun 22, 2036

- GTS Root R2
  Key: RSA 4096
  Serial#: 6e:47:a9:c6:5a:b3:e7:20:c5:30:9a:3f:68:52:f2:6f
  Thumbprint: d2:73:96:2a:2a:5e:39:9f:73:3f:e1:c7:1e:64:3f:03:38:34:fc:4d
  Valid until: Jun 22, 2036

- GTS Root R2
  Key: RSA 4096
  Serial#: 02:03:e5:ae:c5:8d:04:25:1a:ab:11:25:aa
  Thumbprint: 9A:44:49:76:32:DB:DE:FA:D0:BC:FB:5A:7B:17:BD:9E:56:09:24:94
  Valid until: Jun 22, 2036

- GTS Root R3
  Key: ECC 384
  Serial#: 6e:47:a9:c7:6c:a9:73:24:40:89:0f:03:55:dd:8d:1d
  Thumbprint: 30:d4:24:6f:07:ff:db:91:89:8a:0b:e9:49:66:11:eb:8c:5e:46:e5
  Valid until: Jun 22, 2036

- GTS Root R3
  Key: ECC 384
  Serial#: 02:03:e5:b8:82:eb:20:f8:25:27:6d:3d:66
  Thumbprint: ED:E5:71:80:2B:C8:92:B9:5B:83:3C:D2:32:68:3F:09:CD:A0:1E:46
  Valid until: Jun 22, 2036

- GTS Root R4
  Key: ECC 384

Serial#: 6e:47:a9:c8:8b:94:b6:e8:bb:3b:2a:d8:a2:b2:c1:99
Thumbprint: 2a:1d:60:27:d9:4a:b1:0a:1c:4d:91:5c:cd:33:a0:cb:3e:2d:54:cb
Valid until: Jun 22, 2036

- GTS Root R4
  Key: ECC 384
  Serial#: 02:03:e5:c0:68:ef:63:1a:9c:72:90:50:52
  Thumbprint: 77:D3:03:67:B5:E0:0C:15:F6:0C:38:61:DF:7C:E1:3B:92:46:4D:47
  Valid until: Jun 22, 2036
- Root R2
  Key: RSA 2048
  Serial#: 04:00:00:00:00:01:0f:86:26:e6:0d
  Thumbprint: 75:e0:ab:b6:13:85:12:27:1c:04:f8:5f:dd:de:38:e4:b7:24:2e:fe
  Valid until: Dec 15, 2021
- Root R2
  Key: RSA 2048
  Serial#: 02:03:e4:f4:61:ec:99:d9:d5:79:66:ca:7a
  Thumbprint: 02:9D:4B:7E:33:D2:83:8C:66:8C:1D:2C:56:9E:F9:2A:54:0A:7B:96
  Valid until: Dec 15, 2021
- Root R4
  Key: ECC 256
  Serial#: 2a:38:a4:1c:96:0a:04:de:42:b2:28:a5:0b:e8:34:98:02
  Thumbprint: 69:69:56:2e:40:80:f4:24:a1:e7:19:9f:14:ba:f3:ee:58:ab:6a:bb
  Valid until: Jan 19, 2038
- Root R4
  Key: ECC 256
  Serial#: 02:03:e5:7e:f5:3f:93:fd:a5:09:21:b2:a6
  Thumbprint: 6B:A0:B0:98:E1:71:EF:5A:AD:FE:48:15:80:77:10:F4:BD:6F:0B:28
  Valid until: Jan 19, 2038

Prior to 11 August 2016, the Roots R2, R4, GTS Root R1, GTS Root R2, GTS Root R3 and GTS Root R4 were operated by GMO GlobalSign, Inc. according to GMO GlobalSign, Inc.'s Certificate Policy and Certification Practice Statement. Between 11 August 2016 and 8 December 2016, Google Inc. operated these Roots according to Google Inc.'s Certification Practice Statement. As of 9 December 2016, Google Trust Services LLC operates these Roots under Google Trust Services LLC's Certificate Policy and Certification Practice Statement.

The CA certificates of the above listed CAs can be retrieved at https://pki.goog/repository/.

Cross-signed Root CAs

- GTS Root R1
  Key: RSA 4096
  Serial#: 77:bd:0d:6c:db:36:f9:1a:ea:21:0f:c4:f0:58:d3:0d
  Thumbprint: 08:74:54:87:e8:91:c1:9e:30:78:c1:f2:a0:7e:45:29:50:ef:36:f6
  Valid until: Jan 28, 2028

The CA certificates of the above listed CAs can be retrieved at https://pki.goog/repository/.

Intermediate CAs

- GTS CA 1O1
  Key: RSA 2048
  Serial#: 01:e3:b4:9a:a1:8d:8a:a9:81:25:69:50:b8
  Thumbprint: df:e2:07:0c:79:e7:ff:36:a9:25:ff:a3:27:ff:e3:de:ec:f8:f9:c2
  Valid until: Dec 15, 2021
- GTS CA 1D2
  Key: RSA 2048
  Serial#: 01:e3:b4:9d:77:cd:f4:0c:06:19:16:b6:e3
  Thumbprint: 88:4c:fc:da:54:38:5a:12:43:5e:84:7a:5f:6b:16:7a:8c:be:1e:41
  Valid until: Dec 15, 2021
- GTS CA 1C3
  Key: RSA 2048
  Serial#: 02:03:bc:53:59:6b:34:c7:18:f5:01:50:66
  Thumbprint: 1E:7E:F6:47:CB:A1:50:28:1C:60:89:72:57:10:28:78:C4:BD:8C:DC
  Valid until: Sep 30, 2027
- GTS CA 1D4
  Key: RSA 2048
  Serial#: 02:00:8e:b2:02:33:36:65:8b:64:cd:db:9b
  Thumbprint: 34:9C:38:5F:F8:E3:30:F2:0E:AD:73:3C:D3:6F:B4:35:FE:E0:B4:03
  Valid until: Sep 30, 2027
- GTS CA 1P5
  Key: RSA 2048
  Serial#: 02:03:bc:50:a3:27:53:f0:91:80:22:ed:f1
  Thumbprint: 9C:0B:25:2A:67:8A:08:7F:BE:E4:96:A4:43:77:F7:55:6A:C6:05:E7
  Valid until: Sep 30, 2027
- GTS CA 2A1
  Key: ECC 256
  Serial#: 02:00:8e:b2:58:e7:b5:94:0c:1f:f9:00:44
  Thumbprint: 79:03:AF:3E:5C:91:E5:EC:49:71:9B:18:18:0A:91:52:06:71:A1:DC
  Valid until: Sep 30, 2025
- GIAG4
  Key: RSA 2048
  Serial#: 01:f0:9c:57:54:57:97:60:87:2c:7c:24:73
  Thumbprint: bd:1f:9a:24:e0:7d:4b:35:72:6e:d7:f0:65:7a:6f:d9:47:1a:06:72
  Valid until: Dec 15, 2021
- GIAG4x
  Key: RSA 2048
  Serial#: 02:03:f3:58:88:16:16:0e:0a:45:27:f2:a5
  Thumbprint: B6:DB:76:76:B9:A0:32:F2:DD:5F:F5:80:9C:D5:5B:32:87:62:60:CC
  Valid until: Sep 30, 2023

- GIAG4 ECC
  Key: RSA 2048
  Serial#: 01:f0:9c:57:8a:e0:e9:fc:18:55:86:7c:64
  Thumbprint: 67:5c:c5:44:ce:97:be:5f:a8:27:9e:6a:d7:1a:b6:3b:fb:4f:9a:ab
  Valid until: Nov 1, 2028
- GTSY1
  Key: RSA 2048
  Serial#: 01:f0:f7:9d:5e:78:27:fb:40:a9:12:b3:10
  Thumbprint: cd:88:fa:9d:ca:57:2c:5b:8c:3e:ed:3d:a2:e2:62:45:75:46:3f:30
  Valid until: Nov 1, 2028
- GTSY2
  Key: RSA 2048
  Serial#: 01:f0:9c:5b:0e:a2:29:37:cf:9e:e4:41:6c
  Thumbprint: ee:4b:6b:b1:8f:4c:d1:53:2e:59:1a:19:51:39:49:b1:bf:96:a8:fb
  Valid until: Nov 1, 2028
- GTSY3
  Key: ECC 256
  Serial#: 01:fe:a5:80:c2:58:a7:31:cb:c3:b3:9e:ab
  Thumbprint: 76:2c:6a:94:dc:8a:51:34:84:84:9d:6a:60:10:27:7d:0f:ff:97:2a
  Valid until: Nov 1, 2028
- GTSY4
  Key: ECC 256
  Serial#: 01:fe:a5:81:44:7e:3b:fd:3b:b8:1c:24:98
  Thumbprint: 6b:2b:4a:95:87:8c:f5:a9:42:f6:4c:f3:d5:45:f7:70:c8:2b:14:19
  Valid until: Nov 1, 2028

The CA certificates of the above listed CAs can be retrieved at https://pki.goog/repository/.

Externally Operated Subordinate CAs The following (only non-revoked and non-expired) externally operated subordinate CAs have a Google CA listed as the issuer of their CA certificate.

- None

Private CAs, not disclosed to Root Programs

- GTS LTSR
  Key: ECC 256
  Serial#: 01:f0:f7:9d:59:dd:6e:50:f7:42:73:71:50
  Thumbprint: d5:8c:a7:a1:b4:1f:f8:fe:4d:63:7f:ee:ff:ae:50:4a:aa:ff:4f:6f
  Valid until: Nov 1, 2042
- GTS LTSX
  Key: ECC 256
  Serial#: 01:f4:0a:99:c9:b7:a8:55:70:4f:4f:b7:9d
  Thumbprint: 86:01:b1:60:2d:dc:3b:a8:af:b9:92:82:83:d0:d7:d7:70:30:66:83
  Valid until: Apr 1, 2029

1.3.2. Registration authorities

Registration Authorities (RAs) are entities that approve and authenticate requests to obtain, renew, or revoke Certificates. RAs are generally responsible for identifying and authenticating Applicants for Certificates, verifying their authorization to request Certificates, approving individuals, entities, and/or devices to be named in Certificates, and authorizing and/or requesting a CA to issue, renew, or revoke a Certificate to an individual, entity or device.

All RA functions for the Google CAs listed in this CPS are be performed by Google.

1.3.3. Subscribers

Subscribers use Google certificates to support their transactions and communications.

A Subscriber is an individual or organization for whom Google has issued a Certificate on the basis of a Certificate Application. Google may allow Applicants to submit a Certificate Application through the product of a Google Affiliate or directly through an appropriate API. OV certificates include the name of the Subscriber as part of the subject of the certificate.

All Subscribers are required to enter into an agreement that, with respect to each Google Certificate issued to them as a Subscriber, obligates them to:

- Make true representation at all times to Google regarding information in the Certificate and other identification and authentication information requested by Google.
- Maintain possession and control of the Private Key corresponding to the Public Key in the Certificate at all times.
- Implement appropriate security measures to protect their Private Key corresponding to the Public Key included in the Certificate.
- Promptly inform Google of a change to any information included in the Certificate or in the certificate application request.
- Promptly inform Google of any suspected compromise of the Private Key.
- Immediately cease using the Certificate upon expiration of the Certificate, revocation of the Certificate, or in the event of any suspected compromise of the Private Key.
- Use Certificates exclusively for legal purposes and in accordance with this CPS. and in accordance with this CPS.

1.3.4. Relying parties

A Relying Party is any individual or entity that acts in reliance on a Google Certificate to verify a digital signature and/or decrypt an encrypted document or message. Relying Parties may include Google and Google Affiliates, as well as unaffiliated individuals or entities.

1.3.5. Other participants

Not applicable.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Appropriate Certificate uses under this CPS are all uses for the purpose of authentication, using digital signatures, encryption and access control which are consistent with the key usage extension fields of the respective Certificate and are not in violation of the CP, this CPS, applicable law or any agreement made between the Subscriber and Google.

1.4.2. Prohibited certificate uses

Certificates are not proof of the trustworthiness or honesty of the subscriber nor do they indicate the subscriber's compliance with any law. By issuing a certificate Google merely confirms that it has used reasonable means to verify the information in the certificate before it was issued.

Certificates issued under this CPS are not intended and may not be used for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage.

Google certificates may not be used for man-in-the middle purposes or where usage is prohibited by law.

1.5. Policy administration

1.5.1. Organization administering the document

The Google CA Policy Authority is responsible for the drafting, maintenance, and interpretation of this Certification Practice Statement.

1.5.2. Contact person

Google Trust Services LLC
CA Policy Authority
1600 Amphitheatre Parkway
Mountain View, CA 94043
contact@pki.goog

To notify Google of a CA service outage or a security issue including a suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, please contact us using the contact form at https://pki.goog/ or send an email to contact@pki.goog.

If you request a Certificate revocation, please add "Revocation request" and the domain name, IP address or certificate serial number into the subject line of your email.

1.5.3. Person determining CPS suitability for the policy

The Google CA Policy Authority determines the suitability and applicability of this CPS.

1.5.4. CPS approval procedures

Google may change this CPS as deemed necessary. Changes that in the judgment of Google will have no or only a minimal effect on Participants in the Google PKI, may be made without notification. Changes, that in the judgment of Google will have a significant impact on Participants in the Google PKI, will be made with prior notice to such Participants.

CPS changes and potential notifications will be published at https://pki.goog/repository.

A new version of the CPS will become effective fifteen (15) days after it has been published, and will supersede all previous versions and will be binding on all Participants in the Google PKI from that point forward.

1.6. Definitions and acronyms

See Appendix A.

1.6.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements SHALL be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The CAs listed in this CPS are operated by

Google Trust Services LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
contact@pki.goog

2.1. Repositories

Google maintains a Repository which comprises its root certificates, its current CP and CPS, Subscriber Agreements, Relying Party Agreements, and the most recent revocation information for certificates it has issued.

Additionally Google publishes all non-constrained Subordinate CA Certificates and all Cross Certificates it issues including a link to the CPS under which they were issued.

Google represents that it will adhere to the latest version of the CP published in the Repository.

The Repository can be accessed at https://pki.goog/repository/.

Google makes CRLs and OCSP responses for its CAs publicly available through online resources that can be reached 24 hours a day, 7 days a week and are designed to minimize downtime.

CA	CRL
GTS Root R1	http://crl.pki.goog/gtsr1/gtsr1.crl
GTS Root R2	http://crl.pki.goog/gtsr2/gtsr2.crl
GTS Root R3	http://crl.pki.goog/gtsr3/gtsr3.crl
GTS Root R4	http://crl.pki.goog/gtsr4/gtsr4.crl
Root R2	http://crl.globalsign.net/root-r2.crl
Root R4	http://crl.globalsign.net/root-r4.crl

The OCSP responder can be reached under http://ocsp.pki.goog/, as specified in issued certificates.

2.2. Publication of certification information

Web pages that can be used by application software suppliers to test their software with subscriber certificates that chain up to each publicly trusted root certificate are listed at https://pki.goog/repository/.

Google conforms to the current version of the CA/Browser Forum's Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org.

2.3. Time or frequency of publication

CA Certificates are published prior to their usage for issuing to Subscribers.

CRLs are updated promptly upon the revocation of a Certificate, but in no case more than one (1) business day following revocation. The CRLs are periodically updated and reissued at least every seven (7) days, and their validity period is limited to ten (10) days.

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

The Repository is publicly available. Google operates physical and logical security controls to protect the repository from unauthorized modification or deletion.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

OV Certificates contain an X.501 distinguished name in the Subject name field, and incorporate the following attributes:

- Country (C)
- Organization (O)
- Organizational Unit (OU)
- State or Province (ST)
- Locality (L)
- Common Name (CN)

DV Certificates contain an X.501 distinguished name in the Subject name field, and incorporate the following optional attributes:

- Common Name (CN)

Both OV and DV certificates also incorporate the Subject Alternative Name (SAN) extension, which must contain the value of CN from the Subject (if present), and may contain other names that apply to the subject.

3.1.2. Need for names to be meaningful

Domain names included in the CN or SAN attributes must identify one or more specific hosts. Google may issue wildcard Certificates, which identify a set of hosts, as well as Certificates which identify an IP Address.

3.1.3. Anonymity or pseudonymity of subscribers

Subscribers are not permitted to use pseudonyms.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

The CN attribute in root Certificates identifies the publisher and is unique.

3.1.6. Recognition, authentication, and role of trademarks

Certificate Applicants are prohibited from requesting certificates that contain content which infringes on the intellectual property and commercial rights of others. Google does not determine whether Certificate Applicants have intellectual property rights in the name used in a Certificate Application nor does Google resolve any dispute concerning the ownership of a domain name or trademark. Google may reject any Certificate Application and revoke any Certificate because of such a dispute.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The Certificate Applicant must prove ownership of the private key by providing a PKCS #10 compliant certificate signing request, or a cryptographically equivalent proof.

3.2.2. Authentication of organization and domain identity

3.2.2.1. Identity For OV Certificates, the Applicant's identity and its address are validated by using one of the following:

1. A Government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

For S/MIME certificates, Applicant information is validated by using one of the following:

1. An email challenge/response procedure which consists of sending a Random Value to the email address to be included in the Certificate to verify that the Applicant controls the email address.

2. A database maintained by the mail service provider which is periodically updated and considered a Reliable Data Source for identifying authorized certificate requesters.

3. By verifying domain control over the email domain using one of the procedures listed under section 3.2.2.

3.2.2.2. DBA/Tradename Google does not include DBA/Tradenames into Certificates. OV Certificates include the company name of the Subscriber.

3.2.2.3. Verification of Country If the countryName attribute of the subject is present, then Google verifies the country associated with the Subject using one of the following:

1. the IP Address range assignment by country for either
   - the web site's IP address, as indicated by the DNS record for the web site or
   - the Applicant's IP address;
2. the ccTLD of the requested Domain Name;
3. information provided by the Domain Name Registrar; or
4. a method identified in Section 3.2.2.1 of this document.

3.2.2.4. Validation of Domain Authorization or Control Prior to issuing a Certificate, Google validates that the Applicant has control over each FQDN listed in the Certificate by using at least one of the following approved methods as defined in the BR at the time of validation:

- 3.2.2.4.7 DNS Change
- 3.2.2.4.19 Agreed-Upon Change to Website - ACME
- 3.2.2.4.20 TLS Using ALPN

Validation for wildcard domain requests are completed using the DNS Change method.

Google maintains records that indicate which validation method, including relevant BR version number, was used for each domain name.

In addition, Google may supplement its validation procedure with checks against internal data sources.

Google does not issue certificates for FQDNs that contain "onion" as the rightmost label.

3.2.2.5. Authentication of an IP Address IP address authentication is performed in accordance with the procedures set out in Section 3.2.2.5 BR.

For each IP Address listed in a Certificate, Google confirms that, as of the date of Certificate issuance, the Applicant has control over the IP Address by using at least one of the following approved methods as defined in the BR at the time of validation:

- 3.2.2.5.3 Reverse Address Lookup
- 3.2.2.5.6 ACME http-01 method for IP Addresses
- 3.2.2.5.7 ACME tls-alpn-01 method for IP Addresses

Google maintains a record of which IP validation method, including relevant BR version number, was used to validate every IP address.

3.2.2.6. Wildcard Domain Validation Google has established and follows a documented procedure that determines if a wildcard character in a CN or subjectAltName of type DNS-ID occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. ".com“,".co.uk", see RFC 6454 Section 8.2 for further explanation). If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, Google refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7. Data Source Accuracy and Validity Periods All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for I&A purposes.

Data sources are revalidated in accordance with the following terms.

- Legal existence and identity of Applicant - 397 days;
- Domain name - 397 days;
- Authority of Applicant - 397 days.

3.2.2.8. CAA Records Google's policy on checking CAA records is stated in Section 4.2.4.

3.2.3. Authentication of individual identity

Google does not issue IV Certificates to natural persons.

3.2.4. Non-verified Subscriber Information

Google does not include unverified subject information in Subscriber Certificates.

3.2.5. Validation of Authority

Google uses a reliable method of communication with the Applicant or its representative.

The authority of Certificate Applicants to request Certificates on behalf of an organization is verified during the validation of the Applicant's identity.

Google may allow Applicants to specify in writing the individuals who may request Certificates on its behalf. Where such a specification has been made, Google does not accept certificate requests that are outside this specification but will upon written request provide the Applicant a list of its authorized certificate requesters.

3.2.5.1 Verification of Domain Name Ownership For OV certificates, all domain names to be included in a Certificate must be owned by Google or a Google Affiliate. An OV Certificate will not be issued for domain names which do not meet this requirement.

3.2.6. Criteria for Interoperation

All Cross Certificates that identify a Google CA as the Subject are listed in the Repository, provided that Google has arranged for or accepted the establishment of the trust relationship.

3.3. Identification and Authentication for Re-key Requests

I&A procedures for re-key requests are the same as for initial Certificate applications. See Section 3.2.2.

3.3.1. Identification and Authentication for Routine Re-key

See Section 3.2.2.

3.3.2. Identification and Authentication for Re-key after Revocation

See Section 3.2.2.

3.4. Identification and Authentication for Revocation Request

Appropriate identification and authentication procedures are followed when evaluating requests for Certificate Revocation. If revocation is requested by the subscriber, identification and authentication is performed in accordance with Section 3.2. For revocation requests made by a member of Google's Information Security team, identification and authentication is not required.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Applications for an OV Certificate may be submitted by a representative employed by or contracted by, and authorized to act on behalf of, the applicant organization. In addition, applications for a DV Certificate can be submitted by any person through Google's ACME request workflow or through a Google product that offers a certificate request function.

Google maintains an internal database of all previously revoked Certificates and previously rejected certificate requests. That database is used to identify subsequent suspicious certificate requests.

4.1.2. Enrollment process and responsibilities

Applicants seeking to obtain a Google Certificate must submit to Google a certificate application including a certificate request and provide at a minimum, the following:

- The Public Key to be included in the Certificate (if the Subscriber has generated its own Key Pair);
- The fully qualified domain names and/or IP addresses to be included in the Certificate;
- The identity of the Subscriber to be named as the Subject in the Certificate (if the Certificate is to include Subscriber Information);
- An executed Subscriber Agreement, which may be electronic;
- Any other relevant information that Google requests.

One certificate request may be used for multiple Certificates to be issued to the same Applicant.

By executing the Subscriber Agreement, Subscribers warrant that all of the information contained in the certificate request is correct.

4.2. Certificate application processing

Google performs the applicable certificate validation procedures and as required verifies the completeness, accuracy and authenticity of the information provided by the Applicant prior to issuing a Certificate. The procedures include:

- Verifying that the Applicant is permitted to obtain a Certificate under the relevant stipulations of the CP and this CPS.
- Verifying that the Applicant has provided a well-formed, valid certificate signing request, containing a valid signature;
- Obtaining a Public Key from the Applicant;
- Verifying that the Applicant has executed the Subscriber Agreement;
- Validating that the requested Certificate meets the requirements in Sections 3.1.1 - 3.1.5;
- Performing the validation procedures set out in Section 3.2 and the relevant Subsections in so far as they apply to the type of the requested Certificate.

4.2.1. Performing identification and authentication functions

Google performs identification and authentication functions during the Certificate application process.

Certificate Applications are not approved unless Google has obtained all necessary information as specified in Section 4.1.2. If missing information cannot be readily obtained from a trusted internal data source, Google may ask the Applicant to provide the required information in an alternative form.

Data obtained for identification and authentication purposes from a trusted third party source, is confirmed with the Applicant before it is used.

Google maintains procedures to identify High Risk Certificate Requests that require additional verification activity prior to their approval. This includes maintaining an internal database of all Certificates that have previously been revoked and all certificate requests that have been rejected due to suspected phishing or other fraudulent usage or concerns. This information is used during identification and authentication to identify suspicious certificate requests.

4.2.2. Approval or rejection of certificate applications

Google only considers Certificate applications for which all required subscriber information has been provided and validated. All other applications will be rejected.

Certificate applications that contain a new gTLD are not approved while the gTLD is still under consideration by ICANN.

Applications for subordinate CAs are not approved unless the CA in question will be operated by Google or one of its affiliates and will be governed by the CP and this CPS.

4.2.3. Time to process certificate applications

Where Google has entered into a written Service Level Agreement with the Applicant Google will process certificate applications in accordance with the Service Level Objectives defined therein. Otherwise certificate applications will be processed within a reasonable timeframe.

4.2.4. Certificate Authority Authorization (CAA) records

Google checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 8659, following the processing instructions set down in RFC 8659 for any records found.

The following Issuer Domain Names in CAA “issue” or “issuewild” records are recognized as permitting Google to issue:

- pki.goog

If Google issues, it does so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, Google processes the issue, issuewild and iodef property tags as specified in RFC 8659, but does not act on the contents of the iodef property tag.

A Certificate is not issued if an unrecognized property has the critical flag set.

Google may decide not to check for a CAA record:

- For certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked;
- For certificates issued by a Technically Constrained Subordinate CA Certificate as set out in Baseline Requirements Section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.

When checking CAA records, a lookup failure is treated as permission to issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

Google documents potential issuance that was prevented by a CAA record in sufficient detail to provide feedback to the CA/B Forum on the circumstances.

CAA record checking results are logged in certificate lifecycle management event logs (see Section 5.4.1).

URL schemes in the iodef record other than mailto: or https: are not supported.

Google may decide to check for the existence of specific CAA parameters depending on the policy of the certificate that will be issued.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Prior to issuing a Certificate Google processes the Certificate Application and performs the required I&A procedures in accordance with this CPS. Once these procedures have been completed, the Certificate is generated and the appropriate key usage extension added.

Prior to signing a Certificate Google performs conformance linting using appropriate tooling. Linting is done over the precertificate and the issued certificate. If linting reports a nonconformity, a report is generated and issuance is halted.

Certificate Issuance by a root CA requires a CA Engineer to deliberately issue a direct command in order to perform the certificate signing operation.

4.3.2. Notification to subscriber by the CA of issuance of certificate

After issuing the Certificate, Google will notify the Applicant via email or an alternate means of communication and will provide the Applicant with appropriate instructions on how to obtain the Certificate. Delivery of the Certificate will be made via a designated Google service.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The Subscriber indicates acceptance of a Certificate by obtaining it.

By accepting a Certificate, the Subscriber agrees to be bound by the continuing responsibilities, obligations and duties imposed by the Subscriber Agreement and this CPS, and represents and warrants that:

- To its knowledge no unauthorized person has had access to the Private Key associated with the Certificate;
- The information it has supplied during the registration process is truthful and to the extent applicable, has been accurately and fully published within the certificate;
- It will at all times retain control of the Private Key corresponding to the Public Key listed in the Certificate;
- It will immediately inform Google of any event that may invalidate or otherwise diminish the integrity of the Certificate, such as known or suspected loss, disclosure, or other compromise of its Private Key associated with its Certificate.

4.4.2. Publication of the certificate by the CA

Google publishes the CA certificates of all CAs it operates in the Repository.

4.4.3. Notification of certificate issuance by the CA to other entities

Google may notify the public of the issuance of a certificate by submitting it to one or more publicly accessible Certificate Transparency logs.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

4.5.2. Relying party public key and certificate usage

No stipulation.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

Certificate renewal is the process whereby a new Certificate with an updated validity period is created for an existing Key Pair.

As a general rule, Google does not offer Certificate renewal. Whenever a Google Certificate expires, the Subscriber is required to generate a new Key Pair and request a new Certificate in accordance with this CPS.

4.6.2. Who may request renewal

No stipulation.

4.6.3. Processing certificate renewal requests

No stipulation.

4.6.4. Notification of new certificate issuance to subscriber

No stipulation.

4.6.5. Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6. Publication of the renewal certificate by the CA

No stipulation.

4.6.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

Google treats certificate re-key requests as requests for the issuance of a new Certificate.

4.7.2. Who may request certification of a new public key

See Section 4.1.1.

4.7.3. Processing certificate re-keying requests

See Section 4.2.

4.7.4. Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6. Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7. Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8. Certificate modification

Google does not modify previously issued subscriber certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

Google may modify CA Certificates in accordance with the BR and this CPS.

4.8.1. Circumstance for certificate modification

No stipulation.

4.8.2. Who may request certificate modification

See Section 4.1.1.

4.8.3. Processing certificate modification requests

See Section 4.2.

4.8.4. Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate

See Section 4.4.1.

4.8.6. Publication of the modified certificate by the CA

See Section 4.4.2.

4.8.7. Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.9. Certificate revocation and suspension

Google supports Certificate Revocation. Certificate suspension is not used.

When a Certificate is Revoked, it is marked as revoked by having its serial number added to the CRL to indicate its status as revoked. In addition, a signed OCSP response indicating the revoked status is generated.

Certificates that have expired are not revoked.

4.9.1. Circumstances for revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate Google will revoke a Subscriber Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that Google revokes the Certificate;
2. The Subscriber notifies Google that the original certificate request was not authorized and does not retroactively grant authorization;
3. Google obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. Google is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);

5. Google obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name, IP address or email address in the Certificate should not be relied upon.

Google will revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. Google obtains evidence that the Certificate was misused;
3. Google is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
4. Google is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name, IP address or email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. Google is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. Google is made aware of a material change in the information contained in the Certificate;
7. Google is made aware that the Certificate was not issued in accordance with the BR, the CP or this CPS;
8. Google determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. Google's right to issue Certificates under the BR expires or is revoked or terminated, unless Google has made arrangements to continue maintaining its CRL/OCSP Repository;
10. Revocation is required by the CP or this CPS; or
11. Google is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate Google will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies Google that the original certificate request was not authorized and does not retroactively grant authorization;
3. Google obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. Google obtains evidence that the Certificate was misused;
5. Google is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CP or this CPS;
6. Google determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Google or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. Google's or Subordinate CA's right to issue Certificates under the BR expires or is revoked or terminated, unless Google has made arrangements to continue maintaining the CRL/OCSP

Repository; or

9. Revocation is required by the CP and/or this CPS.

4.9.2. Who can request revocation

Certificate Revocation can be requested by:

- The Subscriber or Subject named in the concerned Certificate or its authorized representative;
- Anyone in possession of, or with access to, the Private Key that corresponds to the Public Key in the Certificate;
- Anyone who proves or reasonably suspects that the Private Key which corresponds to the Public Key in the Certificate has been compromised;
- Anyone who proves or reasonably suspects that the certificate has been used fraudulently or in a manner that is otherwise non-compliant with the CP or this CPS;
- Any authorized member of Google's Information Security Team.

4.9.3. Procedure for revocation request

Requests for Certificate revocation and reports concerning suspected certificate misuse, fraud, inappropriate conduct and other certificate related matters can be submitted via email to contact@pki.goog. If the request or report is related to a potential compromise of the private key of a certificate, the requester should also contact security@pki.goog.

Google maintains capabilities to receive Certificate revocation requests 24/7.

Certificate revocation requests that are made by the Subscriber are evaluated using the Identification and Authorization criteria set out in Section 3 of the CP. Requests made by other parties are evaluated on a case by case basis taking into consideration the following criteria:

- The nature of the alleged problem reported by the requestor;
- The evidence provided in support of the request;
- The urgency of the request;
- The quantity of requests received in relation to the concerned Certificate or Subscriber;
- The entity making the request; and
- Applicable legislation.

If Google determines that a revocation is warranted it updates the certificate status information accordingly. Where appropriate Google may also forward the case to law enforcement.

4.9.4. Revocation request grace period

Google may grant revocation grace periods.

4.9.5. Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, Google will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After having investigated the facts and circumstances, Google will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate.

Depending on the revocation reason and as set out in Section 4.9.1., Google will revoke the concerned Certificate no later than 24 hours or 5 days after having received the Certificate Problem Report.

The following criteria will be considered when selecting the revocation date:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint; and
5. Relevant laws and regulations.

4.9.6. Revocation checking requirement for relying parties

Relying Parties are required to confirm the validity of each Certificate in the certificate chain by checking the applicable CRL or OCSP responder before relying on a Google Certificate.

4.9.7. CRL issuance frequency (if applicable)

For the status of Subscriber Certificates: For CAs for which Google publishes a CRL, that CRL is updated and reissued at least once every seven (7) days, and the value of the nextUpdate field is not more than ten (10) days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates: Google updates and reissues 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 is not more than twelve months beyond the value of the thisUpdate field.

See Section 2.2 for CRL locations.

4.9.8. Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9. On-line revocation/status checking availability

Google makes available OCSP status information for all certificates it issues. The OCSP responder locations are included in the respective certificates.

OCSP responses conform to RFC6960 and/or RFC5019. They are either:

1. Signed by the CA that issued the Certificates whose revocation status they indicate, or
2. Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is indicated. The OCSP Responder's signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line revocation checking requirements

The OCSP responder supports GET method for receiving OCSP requests. It does not respond with a "good" status on certificates which have not been issued.

For the status of Subscriber Certificates:

1. OCSP responses have a validity interval greater than or equal to eight hours;
2. OCSP responses have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, Google updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, Google updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates, Google updates information provided via an Online Certificate Status Protocol:

1. at least every twelve months; and
2. within 24 hours after revoking a Subordinate CA Certificate.

4.9.11. Other forms of revocation advertisements available

Not applicable.

4.9.12. Special requirements related to key compromise

In case of a compromise of the Subscriber's private key, the Subscriber must immediately notify Google of the Private Key compromise event. Google will revoke the concerned certificate, and publish a CRL to inform relying parties that the certificate can no longer be trusted.

The subscriber is responsible for investigating the circumstances of any such compromise.

The acceptable methods that can be used by third parties as proof of key compromise are the following:

1. Confirming the third party's possesion of the private key by performing the procedure described in Section 7.6 of RFC 8555 and signing the revocation request with the compromised private key.
2. Confirming the third party's possesion of the private key by signing a challenge provided by Google using the compromised private key.
3. Submitting the private key itself.

4.9.13. Circumstances for suspension

Google does not suspend certificates.

4.9.14. Who can request suspension

Not applicable.

4.9.15. Procedure for suspension request

Not applicable.

4.9.16. Limits on suspension period

Not applicable.

4.10. Certificate status services

4.10.1. Operational characteristics

Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

4.10.2. Service availability

Google operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

Certificate Status Services are available 24x7, unless temporarily unavailable due to maintenance or service failure. Additionally Google maintains a continuous 24x7 ability to respond internally to high-priority Certificate Problem Reports.

4.10.3. Optional features

No stipulation.

4.11. End of subscription

A subscriber's subscription ends when its Certificate expires or when the Certificate is revoked. A subscription also ends when the applicable subscriber agreement expires and is not renewed.

4.12. Key escrow and recovery

Google does not escrow private keys.

4.12.1. Key escrow and recovery policy and practices

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1. Physical controls

The Google CA infrastructure is located in and operated from secure Google facilities. Detailed security procedures are in place and followed that prohibit unauthorized access and entry into the areas of the facilities in which CA systems reside.

5.1.1. Site location and construction

Google CA systems are located in a selected set of locations which have been evaluated for their physical security, as well as local legal considerations that may affect CA operations.

All CA systems are operated from buildings which are solidly constructed to prevent unauthorized entry.

5.1.2. Physical access

Google has in place appropriate physical security controls to restrict access to all hardware and software used for providing CA Services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1. Access is controlled through the use of electronic access controls, mechanical combination lock sets, deadbolts, or other security mechanisms. Such access controls are manually or electronically monitored for unauthorized intrusion at all times. Only authorized personnel will be allowed access, either physical or logical, to the CA systems.

Google enforces two-person access for all access to CA systems.

The Google CA servers are located inside of a locked cabinet or cage area in a locked server room. Access to the server room is controlled by badge readers. The private keys for the CAs are stored in hardware security modules that are validated to FIPS 140-2 Level 3 or higher and that are physically tamper-evident and tamper-resistant.

5.1.3. Power and air conditioning

Google CA facilities are connected to a UPS system and emergency power generator. They are equipped with cooling systems to ensure reliable operations.

5.1.4. Water exposures

All Google CA facilities are equipped with controls which protect CA systems from damage resulting from water leakage.

5.1.5. Fire prevention and protection

All Google CA facilities are equipped with fire detection alarms and protection equipment.

5.1.6. Media storage

No stipulation.

5.1.7. Waste disposal

Google takes reasonable steps to ensure that all media used for the storage of information such as keys, Activation Data or its files are sanitized or destroyed before they are released for disposal.

5.1.8. Off-site backup

Google maintains backup facilities for its CA infrastructure which also hold copies of the CA private keys for redundancy. The backup facilities have security controls which are equivalent to those operated at the primary facility.

5.2. Procedural controls

5.2.1. Trusted roles

All personnel who have access to or control over cryptographic operations of a Google CA that affect the issuance, use, and management of Certificates are considered as serving in a trusted role ("Trusted Role"). Such personnel include, but are not limited to, members of Google's Information Security Team.

5.2.2. Number of persons required per task

CA Private Keys can only be backed up, stored, and recovered by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and authentication for each role

Google maintains controls to provide reasonable assurance that:

- A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed;
- The responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performed is implemented;
- Only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones;
- Individuals in a Trusted Role act only within the scope of such role when required for performing administrative tasks;
- Employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems;
- Trusted Roles use a unique credential created by or assigned to a single person for authentication to Certificate Systems;

- Where Trusted Roles use a username and a password to authenticate, access controls are configured such that at a minimum they satisfy the following requirements:
  - Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones);
  - Passwords for accounts that are accessible from outside a Secure Zone or High Security Zone are configured to have at least eight (8) characters, use a combination of at least numeric and alphabetic characters, and may not be one of the user's previous four passwords; and implement account lockout for failed access attempts; OR
  - Implement a documented password management and account lockout policy that the CA has determined provide at least the same level of protection against password guessing as the foregoing controls.
- Trusted Roles log out of or lock workstations when no longer in use;
- Workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user;
- Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;
- Revoke account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control;
- Disable all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment relationship with the CA;
- Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems;
- Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:
  - The remote connection originates from a device owned or controlled by the CA and from a pre-approved external IP address,
  - The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and
  - The remote connection is made to a designated intermediary device meeting the following:
    - Located within the CA's network,
    - Secured in accordance with these Requirements, and
    - Mediates the remote connection to the Issuing System.

5.2.4. Roles requiring separation of duties

Auditors of the infrastructure and certificate issuance are independent from the operators who approve and issue certificates using a Google CA.

To review their conformance with applicable policies and procedures, Google CAs undergo annual audits performed by independent auditors.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Google has implemented policies for verifying the identity and trustworthiness of its personnel. Furthermore, Google evaluates the performance of its CA staff to ensure that they perform their duties in a satisfactory manner.

All personnel operating the Google CAs are Google employees. There are no contractors or other third parties involved in the Certificate Management Process.

5.3.2. Background check procedures

Google follows a set of established procedures for selecting and evaluating personnel who operate Google CAs or act in other information security roles.

5.3.3. Training requirements

All Google personnel who perform information verification duties receive skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CPS), common threats to the information verification process including phishing and other social engineering tactics.

Validation Specialists receive their skills-training prior to commencing their job role and Google requires them to pass an examination on the applicable information verification requirements.

Google maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain an appropriate skill level.

5.3.4. Retraining frequency and requirements

Google requires personnel in Trusted Roles to maintain skill levels consistent with the CA training and performance management programs. To this end Google requires such personnel to undergo re-training at least annually.

5.3.5. Job rotation frequency and sequence

No stipulation.

5.3.6. Sanctions for unauthorized actions

Google will impose sanctions, including suspension and termination if appropriate, on its employees acting in Trusted Roles if they perform unauthorized acts, abuse their authority, or for other appropriate reasons, at the discretion of the CA management.

5.3.7. Independent contractor requirements

Independent contractors must meet the same training requirements as Google employees working in the same role. Identification and authentication functions are not performed by independent contractors.

5.3.8. Documentation supplied to personnel

Training and documentation is provided to Google employees as necessary for them to perform competently in their job role.

5.4. Audit logging procedures

5.4.1. Types of events recorded

Google records system and CA application events and creates certificate management logs from the data collected in accordance with internal audit procedures. The following events are recorded:

- CA key lifecycle management events
  - Key generation, backup, storage, recovery, archival and destruction;
  - Cryptographic device lifecycle events.
- Applicant and Subscriber events
  - Request to create a certificate;
  - Request to revoke a certificate.
- CA and Subscriber Certificate lifecycle events
  - Verification activities stipulated in the CP and this CPS;
  - Acceptance and rejection of certificate requests, frequency of processing log;
  - Key generation;
  - Key compromise notification;
  - Creation of a certificate;
  - Delivery of a certificate;
  - Revocation of a certificate;
  - Generation of a Certificate Revocation List;
  - Generation of an OCSP response.
- Actions by Trusted Personnel
  - Login events and use of identification and authentication mechanisms;
  - Changes to CA policies;
  - Changes to CA keys;
  - Configuration changes to the CA.
- Security Events
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

Log entries include the following elements:

1. Date and time of entry;

2. Identity of the person making the journal entry; and
3. Description of the entry.

Google collects event information and creates Certificate management logs using automated procedures. Where this is not possible, manual logging and record keeping methods may be used.

5.4.2. Frequency of processing log

Audit logs are reviewed on an as-needed basis.

5.4.3. Retention period for audit log

Google retains generated audit logs for at least seven years, or longer if required by law and makes them available to its Qualified Auditor upon request.

5.4.4. Protection of audit log

Multiple copies of audit logs are stored in different locations and protected by appropriate physical and logical access controls.

5.4.5. Audit log backup procedures

Google maintains formal procedures to ensure that audit logs are backed up and retained to keep them available as necessary for the CA service and as stipulated by applicable standards.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

Events that are deemed potential security issues involving the Certificate Authority infrastructure will be escalated to a permanent security monitoring team.

5.4.8. Vulnerability assessments

On an annual basis, Google's security team performs a Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage caused by these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the adequacy of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

System vulnerabilities are managed in accordance with a formal process that addresses the identification, review, response, and remediation of vulnerabilities.

Additionally, Google performs a Vulnerability Scan on public and private IP addresses belonging to the Certificate Systems on the following occasions:

- Within one week of receiving a request from the CA/Browser Forum;
- After any significant system or network change;
- At least once per quarter.

Google performs a Penetration Test on its Certificate Systems at least once per year and after significant infrastructure changes.

5.5. Records archival

5.5.1. Types of records archived

Records to be archived are those specified in Section 5.4.1.

5.5.2. Retention period for archive

Google retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid, or longer as required by law.

5.5.3. Protection of archive

Archived information is stored at multiple physical locations to protect it from loss.

5.5.4. Archive backup procedures

Backup and recovery procedures exist to ensure that archived information can be restored if it has been lost or destroyed in one storage location.

5.5.5. Requirements for time-stamping of records

Archived records such as log files are time-stamped by the CA systems which generate them. Time-stamps need not be cryptography-based.

5.5.6. Archive collection system (internal or external)

No stipulation.

5.5.7. Procedures to obtain and verify archive information

No stipulation.

5.6. Key changeover

The procedure for providing a new CA Certificate to a Subject following a re-key is the same as the procedure for initially providing the CA Certificate.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

The Google CA infrastructure is operated from redundant production sites. If a disaster causes an outage at one site, the CA service can be provided from an alternate location.

Google maintains an Incident Response Plan and a Disaster Recovery Plan, which set out the procedures necessary to ensure business continuity, to notify affected stakeholders, and to reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. Google annually tests, reviews, and updates its business continuity plan and its security plans and makes them available to its auditors upon request.

The business continuity plan includes:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of involved individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. A plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. A definition of acceptable system outage and recovery times;
13. The frequency at which backup copies of essential business information and software are made;
14. The distance between CA sites; and
15. Procedures for securing an affected facility following a disaster and prior to restoring it either at the original or a different location.

5.7.2. Recovery procedures if computing resources, software, and/or data are corrupted

Redundant CA sites are physically separated. If software or data at one site is corrupted, it can be restored from an alternate site via a secure connection.

Backups of all relevant software and data are made on a regular basis. They are stored off-site and can be retrieved electronically when necessary.

5.7.3. Recovery procedures after key compromise

In the event that the Private Key of a Google CA is compromised, Google will:

- Immediately cease using the compromised key material;
- Revoke all Certificates signed with the compromised key;
- Take commercially reasonable steps to notify all Subscribers of the Revocation; and

- Take commercially reasonable steps to cause all Subscribers to cease using, for any purpose, any such Certificates.

Once the compromised key material has been replaced and a secure operation of the CA in question has been established, the CA may re-issue the revoked certificates following the procedure for initially providing the certificates.

5.7.4. Business continuity capabilities after a disaster

Google employs and contracts security personnel who will use all reasonable means to monitor the CA facility after a natural or other type of disaster so as to protect sensitive materials and information against loss, additional damage, and theft.

To confirm that it possesses appropriate disaster recovery capabilities, Google performs periodic tests of its business continuity and disaster recovery plans.

5.8. CA or RA termination

When it is necessary to terminate operation a Google CA, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. This includes:

- Providing practicable and reasonable prior notice to all Subscribers;
- Assisting with the orderly transfer of service, and operational records, to a successor CA, if any;
- Preserving all records for a minimum of one (1) year or as required by this CPS, whichever is longer; and
- Revoking all Certificates issued by the CA no later than at the time of termination.

If commercially reasonable, prior notice of the termination of a Google CA will be given at least 3 months before the termination date.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

Key Pairs for Google CAs are generated pursuant to formal key generation procedures and inside of a FIPS 140-2 Level 3 certified Hardware Security Module from where the private key cannot be extracted in plaintext.

Requests for Subscriber Certificates are rejected if the Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a Private Key that is known to be weak.

Google does not generate Subscriber Private Keys for TLS server certificates.

6.1.2. Private key delivery to subscriber

Google does not archive Subscriber Private Keys.

6.1.3. Public key delivery to certificate issuer

Subscribers provide their public key to Google for certification through a PKCS#10 Certificate Signing Request. The preferred transfer method for sending this information is HTTP over Transport Layer Security (TLS).

6.1.4. CA public key delivery to relying parties

The public keys of Google CAs are made available from the online Repository at https://pki.goog/repository/. Additionally the public keys of Google root CAs are delivered through their inclusion into the root programs of software and equipment manufacturers.

6.1.5. Key sizes

To prevent cryptanalytic attacks, all Google CAs use key sizes and cryptographic protocols which adhere to NIST recommendations and to the applicable provisions of the CP. See Appendix B for a list of permissible cryptographic algorithms and key sizes.

6.1.6. Public key parameters generation and quality checking

See Appendix B.

6.1.7 Key usage purposes (as per X.509 v3. key usage field)

Root CA Private Keys are not used to sign Certificates except for the following:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

All CA private keys used to sign certificates, CRLs, or any related information leverage hardware security modules meeting FIPS 140-2 Level 3 or higher or Common Criteria EAL4+ security specifications. Cryptography leveraged to protect this information is selected to withstand cryptanalytic attacks for the lifetime of the encrypted key.

CA Private Keys are kept in a physically secure location, and are never stored unencrypted outside of Hardware Security Modules.

6.2.2. Private key (n out of m) multi-person control

All CA Key Pairs are generated in a pre-planned key generation ceremony and in accordance with a written ceremony script. Upon finalization of the ceremony, all participant sign off on the script, and thoroughly record any exceptions that may have occurred in the process.

Ceremony scripts and associated records are retained at least for the lifetime of the generated key pairs.

6.2.3. Private key escrow

The Private Keys of Google CAs are not escrowed.

6.2.4. Private key backup

Backups of CA Private Keys are stored in a secure manner in accordance with applicable Google policy.

6.2.5. Private key archival

Private Keys belonging to Google CAs are not archived by parties other than Google.

6.2.6. Private key transfer into or from a cryptographic module

Private Keys generated on behalf of a Subordinate CA are encrypted for transport to the Subordinate CA.

All transfers of Private Keys into or from a cryptographic module are performed in accordance with the procedures specified by the vendor of the relevant cryptographic module.

6.2.7. Private key storage on cryptographic module

Private keys are stored in accordance with applicable instructions specified by the cryptographic module manufacturer.

6.2.8. Method of activating private key

Private keys are activated in accordance with applicable instructions specified by the cryptographic module manufacturer

6.2.9. Method of deactivating private key

Private keys are deactivated in accordance with applicable instructions specified by the cryptographic module manufacturer.

6.2.10. Method of destroying private key

Private Keys are destroyed in accordance with applicable instructions specified by the cryptographic module manufacturer. In addition Google policy on destruction of highly confidential information is followed.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other aspects of key pair management

6.3.1. Public key archival

No stipulation.

6.3.2. Certificate operational periods and key pair usage periods

Certificates are valid starting at the moment of signing, unless otherwise specified in the certificate validity structure, until the end noted in the certificate expiration time.

Subscriber certificates are issued for a period of one year or less.

6.4. Activation data

6.4.1. Activation data generation and installation

No stipulation.

6.4.2. Activation data protection

Hardware Security Module keys are stored in the Hardware Security Module, and can only be used by authorized CA administrators upon authentication. Passphrases required to unlock the keys are stored in an encrypted form. Physical activation data such as smart cards, when applicable, are stored in a protected and secured environment.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

Google CA system information is protected from unauthorized access through a combination of operating system controls, physical controls and network controls. Network security controls are specified in Section 6.7.

CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2. Computer security rating

No stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

Google uses software that has been formally tested for suitability and fitness for purpose. Hardware is procured through a managed process leveraging industry-standard vendors.

6.6.2. Security management controls

Google has established an Information Security Organization which implements and operates a framework of internal controls that comprises technical, organizational, and procedural measures.

6.6.3. Life cycle security controls

System access is managed on an individual basis and at several levels including the assignment of operating system privileges to the user accounts of individuals performing in Trusted Roles.

6.7. Network security controls

Google's certificate systems are protected by a set of controls that implement the CA/Browser Forum's Network and Certificate System Security Requirements.

These controls include:

- operating hardware firewalls for network perimeter control
- continuously monitoring for system health and security events
- performing regular vulnerability scans and applying system security patches in a timely manner
- managing logical access permissions in accordance with a formal procedure
- enforcing multi-factor authentication
- monitoring the configuration of access permissions
- regularly training all personnel acting in a Trusted Role

6.8. Time-stamping

All logs contain synchronized time stamps.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

Google Certificates conform to RFC 5280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 5280 standard.

Where stipulations of RFC 5280 are in conflict with applicable requirements of the CA/Browser Forum, the CA/Browser Form requirements are followed.

Google generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1. Version number(s)

X.509 Subscriber Certificates issued by Google CAs conform to X.509 version 3.

7.1.2. Certificate extensions

See Appendix C.

7.1.3. Algorithm object identifiers

See Appendix C.

7.1.4. Name forms

7.1.4.1. Encoding For every valid Certification Path (as defined by RFC 5280, Section 6) chaining to a Google Root CA:

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate is byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate is byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2. Subject Information By issuing a Certificate, Google represents that it followed the procedure set forth in Section 3.2 of this CPS to verify that, as of the issuance date, all of the Subject Information was accurate.

Wildcard names may be used for wildcard certificates.

Google's processes relating to I&A and Certificate issuance prevent an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless this information has been verified in accordance with Section 3.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.

All attributes, when present within the subject field, contain information that has been verified.

Subject attributes of SSL certificates do not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that a value is absent, incomplete, or a field is not applicable. dNSName entries are in the "preferred name syntax", as specified in RFC 5280, and do not contain underscore characters ("_").

The commonName of SSL certificates contains a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension.

The commonName of CA certificates is an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy object identifier

Root CA Certificates do not contain the certificatePolicies extension.

End-entity Certificates include one or more of the following Object Identifiers, depending on the method of validation used.

- CA/Browser Forum Baseline Requirements:
  - Domain Validated (DV) Certificates 2.23.140.1.2.1
  - Organization Validated (OV) Certificates 2.23.140.1.2.2
- Google Trust Services Policies:
  - GTS Certificate Policy 1.3.6.1.4.1.11129.2.5.3
  - Signed HTTP Exchanges 1.3.6.1.4.1.11129.2.5.3.1
  - Client Authentication 1.3.6.1.4.1.11129.2.5.3.2
  - Document Signing 1.3.6.1.4.1.11129.2.5.3.3
  - S/MIME 1.3.6.1.4.1.11129.2.5.3.4

7.1.7. Usage of Policy Constraints extension

Certificates do not contain the PolicyConstraints extension.

7.1.8. Policy qualifiers syntax and semantics

No stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2. CRL profile

CRLs issued by Google CAs conform to RFC 5280 standards.

7.2.1. Version number(s)

No stipulation.

7.2.2. CRL and CRL entry extensions

If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, the reasonCode CRL entry extension is present and not marked critical.

If a CRL entry is for a Subscriber Certificate, the reasonCode CRL entry extension subject is present subject to the following requirements.

The CRLReason indicated is not unspecified (0) or certificateHold (6). If the reason for revocation is unspecified, Google omits reasonCode entry extension, if allowed by the previous requirements.

If a reasonCode CRL entry extension is present, the CRLReason indicates the most appropriate reason for revocation of the certificate, as defined by RFC 5280.

7.3. OCSP profile

All Google CAs support OCSP, and their responders conform to the RFC 6960 standard.

If an OCSP response is for a Root CA or Subordinate CA Certificate and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present.

The CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2 of this document.

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

Compliance Audits are conducted at least annually.

8.2. Identity/qualifications of assessor

Compliance audits of Google CAs are performed by a public accounting firm that possesses the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit against the WebTrust Principles and Criteria for Certification Authorities;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Is a licensed WebTrust practitioner;
5. Is bound by law, government regulation, or a professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3. Assessor's relationship to assessed entity

Compliance audits of Google CAs are performed by a public accounting firm that is independent of the subject of the audit.

8.4. Topics covered by assessment

Annual compliance audits of Google CAs include an assessment of the controls Google has implemented to ensure the secure operation of its CAs. In particular they cover an assessment of Google's compliance with the relevant version of the WebTrust Principles and Criteria for Certification Authorities as published by CPA Canada.

8.5. Actions taken as a result of deficiency

If a material deficiency in the design or operation of a control is identified during an audit, Google's CA Policy Authority determines whether remediating actions are required and how these will be implemented. Google seeks the input of its auditor regarding the remediation plans it makes and implements the remediation action within a commercially reasonable period of time.

8.6. Communication of results

The Audit Report is made publicly available no later than three months after the end of the audit period. Google is not required to make publicly available any general audit findings that do not impact the overall audit opinion. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, Google will provide an explanatory letter signed by its Auditor.

The Audit Report states explicitly which CA systems, sites and operational activity it covers.

8.7. Self-Audits

Google monitors its adherence to the CP and this CPS by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

Google requires all Subordinate CAs that it cross signs as well as all Delegated Third Parties to undergo an annual audit which meets the criteria specified in Section 8.1.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

Google may charge Subscribers for the issuance, management and renewal of Certificates. Google does not charge for the revocation of certificates it has issued.

9.1.2. Certificate access fees

Google may charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or status information access fees

Google does not charge a fee as a condition of making the CRLs required by this CPS available in a Repository or otherwise available to Relying Parties. Google may however charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. Google does not permit access to revocation information, Certificate status information, or time stamping in its Repository by third parties that provide products or services that utilize such Certificate status information without Google's prior express written consent.

9.1.4. Fees for other services

Google does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with Google.

9.1.5. Refund policy

No stipulation.

9.2. Financial responsibility

9.2.1. Insurance coverage

Google maintains general liability insurance coverage.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The following Applicant and Subscriber related information is considered confidential information.

1. Certificate applications;
2. Records submitted by the Applicant in support of Certificate applications;
3. Private keys;
4. Log files and other audit records;
5. Transaction records.

9.3.2. Information not within the scope of confidential information

Certificates and revocation data are not considered confidential information. Furthermore information is not considered confidential if its disclosure is mandated pursuant to the CP or this CPS.

9.3.3. Responsibility to protect confidential information

Google, its contractors and agents use a reasonable degree of care when processing and protecting confidential information.

9.4. Privacy of personal information

9.4.1. Privacy plan

Google follows its Privacy Policy which is available at: https://www.google.com/policies/privacy/

9.4.2. Information treated as private

See Section 9.4.1.

9.4.3. Information not deemed private

See Section 9.4.1.

9.4.4. Responsibility to protect private information

See Section 9.4.1.

9.4.5. Notice and consent to use private information

See Section 9.4.1.

9.4.6. Disclosure pursuant to judicial or administrative process

See Section 9.4.1.

9.4.7. Other information disclosure circumstances

See Section 9.4.1.

9.5. Intellectual property rights

Google, or its licensors, own the intellectual property rights in the Google CA services, including the Certificates, trademarks used in providing Certificate services and this CPS.

Certificate and revocation information are the exclusive property of Google. Google grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Google does not allow derivative works of its Certificates or products without prior written permission.

Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the Google Private Keys are the property of Google.

9.6. Representations and warranties

9.6.1. CA representations and warranties

9.6.1.1. Limited warranty Google provides the following limited warranty to the Certificate Beneficiaries at the time of Certificate issuance: (a) it issued the Certificate substantially in compliance with this CPS; b) the information contained within the Certificate accurately reflects the information provided to Google by the Applicant in all material respects; and (c) it has taken reasonable steps to verify that the information within the Certificate is accurate. The steps Google takes to verify the information contained in a Certificate are set forth in this CPS.

9.6.1.2. CABF Warranties and Obligations Domain-validated and organization-validated SSL Certificates conform to the CA/Browser Forum ("CABF") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. By issuing such a Certificate, Google represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, Google has complied with this Section and its CPS in issuing and managing the Certificate.

The Certificate warranties to Certificate Beneficiaries are as follows:

1. Right to Use Domain Name or IP Address: That, at the time of issuance, Google (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the domain name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of domain names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

2. Authorization for Certificate: That, at the time of issuance, Google (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

3. Accuracy of Information: That, at the time of issuance, Google (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

4. No Misleading Information: That, at the time of issuance, Google (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
5. Identity of Applicant: That, if the Certificate contains Subject identity information, Google (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.1.1.1 and 3.2.2.1; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
6. Subscriber Agreement: That, if Subscriber is not a Google Affiliate, the Subscriber and Google are parties to a legally valid and enforceable Subscriber Agreement that satisfies the requirements of this Section, or, if Subscriber is a Google Affiliate, the Applicant acknowledged and accepted Google's Certificate terms of use, notice of which is provided by Google to Applicant during the Certificate issuance process;
7. Status: Google maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. Revocation: Google will revoke the Certificate for any of the reasons specified in this CPS.

9.6.2. RA representations and warranties

No stipulation.

9.6.3. Subscriber representations and warranties

Google requires, as part of the Subscriber Agreement or Terms of Use Agreement, that the Applicant make the commitments and warranties in this Section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, Google obtains, for its express benefit and that of the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

Google implements a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. Google may use an electronic or "click-through" Agreement provided that it has determined that such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

The Subscriber or Terms of Use Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to Google, both in the certificate request and as otherwise requested

by Google in connection with the issuance of the Certificate(s) to be supplied;

2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;
5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request Google to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness: An obligation to respond to Google's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance: An acknowledgment and acceptance that Google is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if Google discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying party representations and warranties

Relying Parties represent and warrant that: (a) they have read, understand and agree to this CPS; (b) they have verified both the relevant Google CA's Certificate and any other certificates in the certificate chain using the relevant CRL or OCSP; (c) they will not use a Certificate if the Certificate has expired or been revoked; (d) they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate; (e) they have studied the applicable limitations on the usage of Certificates and agree to Google's limitations on liability related to the use of Certificates; (f) they are solely responsible for deciding whether or not to rely on information in a Certificate; and (g) they are solely responsible for the legal and other consequences of their failure to perform the Relying Party obligations in this CPS.

Relying Parties also represent and warrant that they will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:

1. Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

2. The intended use of the Certificate as listed in the Certificate or this CPS;

3. The data listed in the Certificate;

4. The economic value of the transaction or communication;
5. The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication;
6. The Relying Party's previous course of dealing with the Subscriber;
7. The Relying Party's understanding of trade, including experience with computer-based methods of trade; and
8. Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE.” TO THE MAXIMUM EXTENT PERMITTED BY LAW, GOOGLE DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO CERTIFICATES ISSUED BY GOOGLE, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN THE GOOGLE PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANY OTHER GOODS OR SERVICES PROVIDED BY GOOGLE TO THE PARTICIPANT.

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, GOOGLE DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

Google does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an individual or entity uses Google's services.

9.8. Limitations of liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, GOOGLE SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOST DATA, LOST PROFITS, LOST REVENUE OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT OR TORT (INCLUDING PRODUCTS LIABILITY, STRICT LIABILITY AND NEGLIGENCE), AND WHETHER OR NOT IT WAS, OR SHOULD HAVE BEEN, AWARE OR ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF

ANY LIMITED REMEDY STATED HEREIN. GOOGLE'S AGGREGATE LIABILITY UNDER THIS CPS IS LIMITED TO $500.

9.9. Indemnities

To the extent permitted by applicable law, Relying Parties shall indemnify Google for their: (a) violation of any applicable law (b) breach of representations and obligations as stated in this CPS; (c) reliance on a Certificate that is not reasonable under the circumstances; or (d) failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10. Term and termination

9.10.1. Term

The CPS becomes effective upon publication in the Repository. Amendments to this CPS become effective upon publication in the Repository.

9.10.2. Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of termination and survival

Upon termination of this CPS, Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.11. Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12. Amendments

9.12.1. Procedure for amendment

Google may change this CPS at any time in its sole discretion and without prior notice to Subscribers or Relying Parties. The CPS and any amendments thereto are available in the Repository. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

9.12.2. Notification mechanism and period

Google may provide additional notice (such as in the Repository or on a separate website) in the event that it makes any material changes to its CPS. Google is responsible for determining what constitutes a material change of the CPS. Google does not guarantee or set a notice-and-comment period.

9.12.3. Circumstances under which OID must be changed

No stipulation.

9.13. Dispute resolution provisions

No stipulation

9.14. Governing law

This CPS is governed by the laws of the State of California of the United States of America, excluding (i) its choice of laws principles, and (ii) the United Nations Convention on Contracts for the International Sale of Goods. All Participants hereby submit to the exclusive jurisdiction and venue of the federal or state courts in Santa Clara County, California.

9.15. Compliance with applicable law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. Google licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Assignment

Relying Parties and Subscribers may not assign their rights or obligations under this CPS, by operation of law or otherwise, without Google's prior written approval. Any such attempted assignment shall be void. Subject to the foregoing, this CPS shall be binding upon and inure to the benefit of the parties hereto, their successors and permitted assigns.

9.16.3. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Google may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Google's failure to enforce a provision of this CPS does not waive Google's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by Google.

9.16.5. Force Majeure

Google shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Google.

9.17. Other provisions

No stipulation.

Appendix A: Definitions, Acronyms and References

Definitions

Automatic Certificate Management Environment (ACME): A communications protocol for automating interactions between Certificate Authorities and their Subscribers.

Activation Data: Data, other than keys, that is required to access or operate cryptographic modules (e.g., a passphrase or a Personal Identification Number or "PIN").

API: An interface that allows users to programmatically access the features of a system, application, or service.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the audit opinion.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of the BR.

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

Baseline Requirements (BR): CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, available at https://cabforum.org/baseline-requirements-documents/

CAA: From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

CA Services: Services relating to the creation, issuance, or management of Certificates provided by Google under this CPS.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certification Authority (CA): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs. The term CA can depending on the context also refer to the infrastructure used by that organization to provide CA Services.

Client Authentication Certificate: A Certificate intended to be issued to individuals (as well as devices not acting in the capacity of a server), solely for the purpose of identifying that the holder of the Private Key is in fact the individual or device named in the Certificate's subject field.

Certificates: The Certificates that a Google CA is authorized to issue pursuant to this CPS. See Google Certificate.

Certificate Beneficiaries: any of the following parties:

(i) The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;

(ii) all Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and

(iii) all Relying Parties who reasonably rely on a valid Certificate.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certification Practice Statement (CPS): This document.

Certificate Policy (CP): Google's Certificate Policy.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List (CRL): A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

CN: Common Name

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.

CSPRNG: A random number generator intended for use in cryptographic system.

DBA: Doing Business As

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Validated (DV) Certificate: A Certificate which verifies that the Subscriber controls the domain names and IP addresses included in the Certificate.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Fully-Qualified Domain Name (FQDN): A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

FIPS: (US Government) Federal Information Processing Standard

Google: Google Trust Services LLC (a Delaware corporation).

Google Affiliate: An entity that is controlled with or by or is under common control with Google.

Google CA: A CA operated by Google in accordance with this CPS and listed in Section 1.3.1 of this CPS.

Google Certificate: A certificate issued by a Google CA under this CPS.

Google PKI: The Google Public Key Infrastructure established, operated and maintained by Google for publicly trusted certificates.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Identification and Authentication (I&A): The process for ascertaining and confirming through appropriate inquiry and investigation the identity and authority of a person or entity. See Section 3.2

Incorporating Agency: The government agency in the jurisdiction in which an entity is incorporated under whose authority the legal existence of the entity was established (e.g., the government agency that issued the Certificate of Incorporation).

Individual Validated (IV) Certificate: A Certificate which has been issued to a natural person and includes the Subscriber's name.

Information Security Team: Google employees who belong to the Privacy & Security organization.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP Address: A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Pair: Two mathematically related numbers, referred to as a Public Key and its corresponding Private Key, possessing properties such that: (i) the Public Key may be used to verify a Digital Signature generated by the corresponding Private Key; and/or (ii) the Public Key may be used to encrypt an electronic record that can be decrypted only by using the corresponding Private Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

NIST: (US Government) National Institute of Standards and Technology

OCSP: Online Certificate Status Protocol

OID: Object Identifier

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Operational Period: The intended term of validity of a Google Certificate, including beginning and ending dates. The Operational Period is indicated in the Certificate's "Validity" field. See also Expire.

Organization Validated (OV) Certificate: A Certificate which includes the Subscriber's organization name.

Participants: The persons authorized to participate in the Google PKI, as identified in Section 1.3. This term includes the Google CAs, and each Subscriber and Relying Party operating under the authority of the Google PKI.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Cryptography: A type of cryptography, also known as asymmetric cryptography, that uses a unique Key Pair in a manner such that the Private Key of that Key Pair can decrypt an electronic record encrypted with the Public Key, or can generate a digital signature, and the corresponding Public Key, to encrypt that electronic record or verify that Digital Signature.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

RA: See Registration Authority.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Registration Process: The process, administered by the CA or an RA, that a Subscriber uses to apply for and obtain a Google Certificate.

Reissuance: The process of acquiring a new Google Certificate and associated Key Pair to replace an existing Google Certificate and associated Key Pair, prior to the Expiration of the existing Google Certificate and associated Key Pair's Operational Period.

Relying Party: A recipient of a Certificate who acts in reliance on the Certificate and/or digital signatures verified using the Certificate.

Repository: An online accessible database in the Google PKI containing this CPS, the CRL for revoked Google Certificates, and any other information specified by Google.

Request Token: A value derived in a method specified by the CA and used to demonstrate domain control.

The Request Token incorporates the key used in the certificate request.

A Request Token may include a timestamp to indicate when it was created and other information to ensure its uniqueness.

A Request Token that includes a timestamp remains valid for no more than 30 days from the time of creation and is treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and Google does not re-use it for a subsequent validation.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

- http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
- http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Revocation: The process of requesting and implementing a change in the status of a Certificate from valid to Revoked.

Revoked: A Certificate status designation that means the Certificate has been rendered permanently Invalid.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: The individual or organization that is named as the Subject of a Certificate and that has agreed to the terms of a Subscriber Agreement with Google.

Subscriber Agreement: The contract between Google and a Subscriber whereby the Subscriber agrees to the terms required by this CPS with respect to each Certificate issued to the Subscriber and naming the Subscriber as the Subject.

Subsidiary Company: A company that is controlled by or under common control of a Parent Company.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

TLS: Transport Layer Security

Token: A hardware device (such as a smart card) used to store a Key Pair and associated Certificate and to perform cryptographic functions.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed by a single full stop character (”*.”) followed by a Fully-Qualified Domain Name.

Acronyms

AICPA, American Institute of Certified Public Accountants

CA, Certificate Authority

CAA, Certificate Authority Authorization

ccTLD, Country Code Top-Level Domain

CICA, Canadian Institute of Chartered Accountants

CP, Certificate Policy

CPS, Certification Practice Statement

CRL, Certificate Revocation List

DBA, Doing Business As

DNS, Domain Name System

FIPS, (US Government) Federal Information Processing Standard

FQDN, Fully Qualified Domain Name

IM, Instant Messaging

IANA, Internet Assigned Numbers Authority

ICANN, Internet Corporation for Assigned Names and Numbers

ISO, International Organization for Standardization

NIST, (US Government) National Institute of Standards and Technology

OCSP, Online Certificate Status Protocol

OID, Object Identifier

PKI, Public Key Infrastructure

RA, Registration Authority

S/MIME, Secure MIME (Multipurpose Internet Mail Extensions) SSL Secure Sockets Layer

TLD, Top-Level Domain

TLS, Transport Layer Security

VOIP, Voice Over Internet Protocol

References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

Internet Draft: ACME IP Identifier Validation Extension, R. Shoemaker, July 2018, https://tools.ietf.org/html/draft-ietf-acme-ip-04.

ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework. Network and Certificate System Security Requirements, v.1.0, 1/1/2013.

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf.

RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.

RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.

RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.

RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

RFC7301, Request for Comments: 7301, Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension. Friedl, Popov, Langley, Stephan, July 2014.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, Hoffman-Andrews, November 2019.

RFC8737, Request for Comments: 8737, Automated Certificate Management Environment (ACME) TLS Application-Layer Protocol Negotiation (ALPN) Challenge Extension. Shoemaker, February 2020.

WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.2, available at http://www.webtrust.org/principles-and-criteria/docs/item83987.pdf.

X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Appendix B: Permissible Cryptographic Algorithms and Key Sizes

The following algorithms and key lengths are permissible for subscriber certificates:

Type	Permissible values
Digest Algorithm	SHA-256, SHA-384 or SHA-512
RSA	2048 bits or longer
ECC	NIST P-256, P-384

The following additional requirements apply to RSA keys:

1. the public exponent must be an odd number equal to 3 or more,
2. the public exponent is in the range between 2^16 + 1 and 2^256 - 1,
3. the modulus size, when encoded, is at least 2048 bits,
4. the modulus size, in bits, is evenly divisible by 8,
5. the modulus is an odd number,
6. the modulus is not the power of a prime, and
7. the modulus has no factors smaller than 752.

The validity of all ECDSA keys is confirmed using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine.

Appendix C: Google Certificate Profiles

This appendix sets out the Profiles of Certificates issued from Google CAs. Fields and extensions not mentioned herein shall be set in accordance with RFC 5280.

Google does not issue Certificates that contain a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in the corresponding certificate profile unless it is aware of a reason for including the data in the respective Certificate.

Moreover Google does not issue Certificates with:

1. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
    1. such value falls within an OID arc for which the Applicant demonstrates ownership, or
    2. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
2. semantics that, if included, will mislead a Relying Party about the certificate information verified by the Google Internet Authority (such as including extendedKeyUsage value for a smart card, where the Google Internet Authority is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).
3. Internal Names or Reserved IP Addresses in the Common Name or Subject Alternative Name field.

The following EKUs may be enabled:

- Server Authentication = 1.3.6.1.5.5.7.3.1
- Client Authentication = 1.3.6.1.5.5.7.3.2
- Secure E-mail EKU = 1.3.6.1.5.5.7.3.4

Certificates do not combine server authentication with code signing uses unless the uses are separated by application of Extended Key Usages (“EKU”s) at the intermediate CA certificate level that are reflected in the whole certificate chain.

Algorithm object identifiers

Effective 1 January 2016, Google does not issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm.

SubjectPublicKeyInfo

RSA Google indicates an RSA key using the rsaEncryption (OID: 1.2.840.113549.1.1.1) algorithm identifier. The parameters are be present, and are an explicit NULL. Google does not use a different algorithm to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys is byte-for-byte identical with the following hex-encoded bytes: 300d06092a864886f70d0101010500

ECDSA Google indicates an ECDSA key using the id-ecPublicKey (OID: 1.2.840.10045.2.1) algorithm identifier. The parameters use the namedCurve encoding.

1. For P-256 keys, the namedCurve is secp256r1 (OID: 1.2.840.10045.3.1.7).
2. For P-384 keys, the namedCurve is secp384r1 (OID: 1.3.132.0.34).

When encoded, the AlgorithmIdentifier for ECDSA keys is byte-for-byte identical with the following hex-encoded bytes:

1. For P-256 keys, 30 13 06 07 2a 86 48 ce 3d 02 01 06 08 2a 86 48 ce 3d 03 01 07.
2. For P-384 keys, 30 10 06 07 2a 86 48 ce 3d 02 01 06 05 2b 81 04 00 22.

Signature AlgorithmIdentifier

All objects signed by a Google CA Private Key conform to the following requirements on the use of the AlgorithmIdentifier or AlgorithmIdentifier-derived type in the context of signatures.

In particular, the requirements appliy to all of the following objects and fields:

1. The signatureAlgorithm field of a Certificate or Precertificate.
2. The signature field of a TBSCertificate (for example, as used by either a Certificate or Precertificate).
3. The signatureAlgorithm field of a CertificateList
4. The signature field of a TBSCertList
5. The signatureAlgorithm field of a BasicOCSPResponse.

No other encodings are used for these fields.

RSA Google uses one of the following signature algorithms and encodings. When encoded, the AlgorithmIdentifier is byte-for-byte identical with the specified hex-encoded bytes.

1. RSASSA-PKCS1-v1_5 with SHA-256: Encoding: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00.
2. RSASSA-PKCS1-v1_5 with SHA-384: Encoding: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0c 05 00.
3. RSASSA-PKCS1-v1_5 with SHA-512: Encoding: 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0d 05 00.
4. RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes: Encoding: 30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 a2 03 02 01 20
5. RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes: Encoding: 30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 02 05 00 a2 03 02 01 30
6. RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes: Encoding: 30 41 06 09 2a 86 48 86 f7 0d 01 01 0a 30 34 a0 0f 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 a1 1c 30 1a 06 09 2a 86 48 86 f7 0d 01 01 08 30 0d 06 09 60 86 48 01 65 03 04 02 03 05 00 a2 03 02 01 40

ECDSA Google uses the appropriate signature algorithm and encoding based upon the signing key used.

1. If the signing key is P-256, the signature MUST use ECDSA with SHA-256. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 30 0a 06 08 2a 86 48 ce 3d 04 03 02.
2. If the signing key is P-384, the signature MUST use ECDSA with SHA-384. When encoded, the AlgorithmIdentifier MUST be byte-for-byte identical with the following hex-encoded bytes: 30 0a 06 08 2a 86 48 ce 3d 04 03 03.

Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, is not considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Root CA Certificate

Field	Content
issuer	Matches subject
validity:not after	At least 8 but less or equal to 25 years after the certificate was issued or the validity:notBefore date – whichever is later.
subject	Contains countryName, organizationName and commonName. commonName attribute identifies the publisher, is unique, readable and in a language appropriate for the market of the respective CA.
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:basicConstraints	marked critical, cA is TRUE
extension:keyUsage	marked critical, keyCertsign and cRLSign are set, digitalSignature may be set, other bits are not set

Subordinate TLS CA Certificate

Field	Content
validity:not after	Not later than notAfter date of signing certificate
subject	Contains countryName, organizationName and commonName
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present

Field	Content
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	marked critical, cA is TRUE, pathLenConstraint field may be present
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:keyUsage	marked critical, keyCertsign, and cRLSign bits are set, digitalSignature may be set, all other bits are not set
extension:authorityInfoAccess	not marked critical, contains HTTP URL of the Issuing CA's certificate and the HTTP URL of Issuing CA's OCSP responder
extension:extkeyUsage	not marked critical, must include id-kp-serverAuth; may include id-kp-clientAuth; must not include id-kp-emailProtection, id-kp-codeSigning, id-kp-timeStamping or anyExtendedKeyUsage; should not include other values [RFC 5280]

Subordinate S/MIME CA Certificate

Field	Content
validity:not after	Not later than notAfter date of signing certificate
subject	Contains countryName, organizationName and commonName
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	marked critical, cA is TRUE, pathLenConstraint field may be present
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:keyUsage	marked critical, keyCertsign, and cRLSign bits are set, digitalSignature may be set, all other bits are not set
extension:extkeyUsage	not marked critical, id-kp-emailProtection must be set, should not include other values [RFC 5280]
extension:authorityInfoAccess	not marked critical, contains the HTTP URL of the Issuing CA's certificate and the HTTP URL of Issuing CA's OCSP responder
extension:nameConstraints	optional. if present, marked critical, contains at least one permittedSubtrees field [RFC 5280]

Organization Validation TLS Certificate

Field	Content
validity:not after	Not more than 365 days after the later of validity:notBefore or the date the certificate was issued
subject	Contains countryName, locality (to the extent such field is required under Section 7.1.4.2.2 BR), stateOrProvinceName (to the extent such field is required under Section 7.1.4.2.2 BR), organizationName. May contain commonName, may contain organizationUnit. If the subject contains a commonName attribute, the value must be one of the values in the subjectAlternativeName extension.
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains the HTTP URL of the Issuing CA's certificate and the HTTP URL of Issuing CA's OCSP responder
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 5280]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	not marked critical, must contain at least one name and all names must be of type dNSName or iPAddress
extension:keyUsage	optional. if present, marked critical, digitalSignature bit must be set, nonRepudiation, keyEncipherment or keyAgreement may be set, other bits are not set.
extension:extkeyUsage	not marked critical, must include either id-kp-serverAuth or id-kp-clientAuth, or both [RFC 5280]

Domain Validation TLS Certificate

Field	Content
validity:not after	Not more than 365 days after the later of validity:notBefore or the date the certificate was issued
subject	May be an empty sequence. May contain commonName. Must not contain other attributes. If the subject contains a commonName attribute, the value must be one of the values in the subjectAlternativeName extension.
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains HTTP URL of the Issuing CA's certificate and the HTTP URL of Issuing CA's OCSP responder
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 5280]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	must contain at least one name and all names must be of type dNSName or iPAddress. Must be marked critical if Subject is empty, not marked critical otherwise.
extension:keyUsage	optional. if present, marked critical, digitalSignature bit must be set, nonRepudiation, keyEncipherment or keyAgreement may be set, other bits are not set.
extension:extkeyUsage	not marked critical, must include either id-kp-serverAuth or id-kp-clientAuth, or both [RFC 5280]

Signed HTTP Exchange Certificate

Field	Content
validity:not after	Not more than 90 days after the later of validity:notBefore or the date the certificate was issued

Field	Content
subject	May be an empty sequence. May contain commonName. If the subject contains a commonName attribute, the value must be one of the values in the subjectAlternativeName extension.
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 5280]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains HTTP URL of the Issuing CA's certificate and the HTTP URL of Issuing CA's OCSP responder
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 5280]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	must contain at least one name and all names must be of type dNSName. Must be marked critical if Subject is empty, not marked critical otherwise.
extension:keyUsage	optional. if present, marked critical, digitalSignature bit must be set, nonRepudiation, keyEncipherment or keyAgreement may be set, other bits are not set.
extension:extkeyUsage	not marked critical, must include either id-kp-serverAuth or id-kp-clientAuth, or both [RFC 5280]
extension:canSignHttpExchanges	not marked critical, must have the value NULL

S/MIME Certificate

Field	Content
validity:not after	Not more than 365 days after the later of validity:notBefore or the date the certificate was issued
subject	empty
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 5280]

Field	Content
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains HTTP URL of the Issuing CA's certificate
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 5280]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	marked critical, must contain at least one name and all names must be of type rfc822Name.
extension:keyUsage	marked critical, digitalSignature bit must be set, other bits are not set.
extension:extkeyUsage	not marked critical, id-kp-emailProtection must be set, should not include other values [RFC 5280]

Appendix D: Document History

Version	Date	Change owner	Note
1.0	2016-12-09	CA Policy Authority	Initial publication
1.1	2016-12-14	CA Policy Authority	Updated certificate profiles
1.2	2016-12-27	CA Policy Authority	Added additional note on previous operation of R2 and R4
1.3	2017-01-11	CA Policy Authority	Added additional note on previous operation of Root CAs
1.4	2017-02-15	CA Policy Authority	Updated contact information
1.5	2017-02-26	CA Policy Authority	Added GIAG3 subordinate
1.6	2017-04-07	CA Policy Authority	Removed revoked EV/G2 subCAs
1.7	2017-05-29	CA Policy Authority	Updated certificate profiles and OCSP terms
1.8	2017-06-16	CA Policy Authority	Added new subCAs created in 2017-06-15 ceremony
1.9	2017-09-08	CA Policy Authority	Aligned with new version of CA/B Forum Requirements
2.0	2017-12-04	CA Policy Authority	Updated Section on Certificate Validation
2.1	2018-01-31	CA Policy Authority	Clarified contact information
2.2	2018-03-08	CA Policy Authority	Wording improvements
2.3	2018-08-01	CA Policy Authority	Replaced method for validation of domain authorization or control
2.4	2018-08-24	CA Policy Authority	Updated permissible crypto algorithms
2.5	2018-09-11	CA Policy Authority	Added BR references for IP address authentication
2.6	2018-10-23	CA Policy Authority	Updated revocation timelines as per CA/B Forum Ballot SC6
2.7	2018-11-06	CA Policy Authority	Added new CAs created in 2018-10-29 ceremony
2.8	2019-01-07	CA Policy Authority	Added prohibition of underscore characters in dNSName entries

Version	Date	Change owner	Note
2.9	2019-04-05	CA Policy Authority	Update LTSX info
2.10	2019-05-08	CA Policy Authority	Updates for DV issuance
2.11	2019-05-20	CA Policy Authority	General updates and wording improvements
2.12	2019-08-01	CA Policy Authority	Updated IP Address validation methods
2.13	2019-09-30	CA Policy Authority	Updated certificate profile definitions
2.14	2019-10-02	CA Policy Authority	Removed revoked GIAG3, GTSX and GlobalSign EV CA G2 subCAs
2.15	2020-01-31	CA Policy Authority	Updated re-issued GTSY3 and GTSY4
2.16	2020-02-03	CA Policy Authority	Updated section on indemnities
2.17	2020-06-02	CA Policy Authority	Updated validation methods in Section 3.2.2.4
2.18	2020-06-18	CA Policy Authority	Added GTS Root R1 cross sign
2.19	2020-07-28	CA Policy Authority	Updated certificate profiles for SXG issuance
2.20	2020-08-06	CA Policy Authority	Distinguished between Subscriber- and CA Certificates in Section 4.8
2.21	2020-08-13	CA Policy Authority	Added reissued roots and new subCAs created in 2018-08-13 ceremony
2.22	2020-08-21	CA Policy Authority	Removed obsolete Google PKI Policy OID in Section 7.1.6
3.0	2021-03-19	CA Policy Authority	Updated various sections following annual CPS review
3.1	2021-04-07	CA Policy Authority	Added methods that can be used as proof of private key compromise
3.2	2021-04-13	CA Policy Authority	Added ACME IP Address validation methods
3.3	2021-04-22	CA Policy Authority	Remove 3.2.2.4.10 as a validation method
3.4	2021-04-26	CA Policy Authority	Add 3.2.2.4.20 as a validation method
4.0	2021-08-11	CA Policy Authority	Updated various sections following full CPS review