Google Trust Services, Certification Practice Statement v1.8

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 in response to Google's Certificate Policy and sets forth the practices that Google has adopted to implement the provisions made therein.

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, SHA-384
  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 R2
  Key: RSA 4096, SHA-384
  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 R3
  Key: ECC 384, SHA-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 R4
  Key: ECC 384, SHA-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
- Root R2
  Key: RSA 2048, SHA-1
  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 R4
  Key: ECC 256, SHA-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

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 http://pki.goog/.

Intermediate CAs

- GTS X1
  Key: RSA 2048, SHA-256
  Serial#: 6e:47:a9:c9:a5:53:e3:c2:ce:1f:14:4e:d7:7d:ac:e7
  Thumbprint: 0f:d1:f2:00:9d:51:01:1d:23:f8:72:96:27:90:d1:c8:23:44:33:6f
  Valid until: Jun 22, 2026
- GTS X2
  Key: RSA 2048, SHA-256
  Serial#: 6e:47:a9:ca:ce:7f:84:65:19:2e:e7:33:2b:27:27:c3
  Thumbprint: 29:35:6c:48:6b:b0:e2:ec:8a:0f:c9:0b:ed:73:b8:fa:1d:c1:13:df
  Valid until: Jun 22, 2026
- GTS X3
  Key: RSA 2048, SHA-256
  Serial#: 6e:47:a9:cc:b4:5a:29:c7:b0:78:d0:1b:a3:21:12:61
  Thumbprint: c1:dd:09:28:69:8b:06:c6:fb:1f:7c:db:10:03:d8:7b:51:26:11:ae
  Valid until: Jun 22, 2026
- GTS X4
  Key: RSA 2048, SHA-256
  Serial#: 6e:47:a9:ce:4f:46:c2:3d:e2:49:ea:cc:38:94:53:73

Thumbprint: e0:fb:04:9e:23:c6:59:20:8b:62:33:68:a0:d2:61:e3:9a:42:18:b2
Valid until: Jun 22, 2026

- GIAG3
  Key: RSA 2048, SHA-256
  Serial#: 30:12:9b:fd:80:d1:93:d6:b3:e2:34:e4
  Thumbprint: 31:36:88:50:36:18:ae:78:17:b5:05:75:c5:a6:26:94:24:f9:ce:6e
  Valid until: Dec 15, 2021
- GIAG3
  Key: RSA 2048, SHA-256
  Serial#: 01:e3:a9:30:1c:fc:72:06:38:3f:9a:53:1d
  Thumbprint: ee:ac:bd:0c:b4:52:81:95:77:91:1e:1e:62:03:db:26:2f:84:a3:18
  Valid until: Dec 15, 2021
- GIAG3 ECC
  Key: ECC 256, SHA-256
  Serial#: 01:e3:ae:80:26:db:5b:41:e2:56:c2:a3:51
  Thumbprint: e0:f8:0b:f7:01:28:7c:00:51:00:c9:15:c9:f4:3b:21:19:d9:cf:96
  Valid until: Jun 15, 2027
- GTS CA 1O1
  Key: RSA 2048, SHA-256
  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, SHA-256
  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

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

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.

- GlobalSign Extended Validation CA - SHA256 - G2
  Key: RSA 2048, SHA-256
  Serial#: 04:00:00:00:00:01:44:4e:f0:4a:55
  Thumbprint: 65:be:10:2b:e2:69:28:65:0e:0e:f5:4d:c8:f4:f1:5a:f5:f9:8e:8b
  Valid until: Dec 15, 2021
  Cross Certified: February 2014
  Certificate: DER

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 will be performed by Google.

1.3.3. Subscribers

A Subscriber is an individual or an organization capable of using, and authorized to use, the Private Key that corresponds to the Public Key listed in a Certificate, and that: (1) is named in a Certificate's "Subject" field, and (2) has agreed to the terms of a Subscriber Agreement with Google.

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

The Google CAs listed in this CPS are operated by Google Inc on behalf of Google Trust Services LLC.

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

For security issues, such as vulnerability reports or external reports of key compromise, please contact security@pki.goog.

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 notofications will be published at http://pki.goog/.

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.

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 http://pki.goog/.

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 hosted at http://pki.goog/.

Google's practice with regards to CAA records is stated in section 4.2.4.

2.2. Publication of certification information

Google makes CRLs and OSCP 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

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

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

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 (S)
- Locality (L)
- Common Name (CN)
- E-mail Address (E)

Certificates also incorporate the Subject Alternative Name (SAN) attribute, which repeats the Common Name, as well as any other names that may 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.

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 is infringing 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. This requirement does not apply when a key pair is generated by Google on behalf of the Applicant.

3.2.2. Authentication of organization identity

Google follows the CP when authenticating the identity of organizations.

Identification and Authentication ("I&A") procedures are performed on all Applicants, and on all persons, entities, devices, and domains to be named in a Certificate, in the following circumstance:

- During the Certificate application process
- During the Certificate re-key process

I&A procedures ensure that all Applicants for Google Certificates, and all Subject information to be included in the Certificate, conform to the requirements of, and have been verified in accordance with this CPS. Such verification processes are intended to accomplish the following:

- Verify the identity of the Applicant applying for the Google Certificate
- Verify the existence and identity of the Subject;
- Verify the Subject's physical location (presence at a physical address);
- Verify the Subject's ownership of (or exclusive right to control) the domain name to be included in the Certificate (where applicable);
- Verify the Subject's ownership and control of, the device name to be included in the Certificate (where applicable);
- Verify the Applicant's authorization to apply for the Certificate.

3.2.2.1. Identity

Google follows the CP when verifying the identity of Certificate Applicants.

3.2.2.2. DBA/Tradename

Google follows the CP when verifying that the Applicant holds the right to use a DBA/Tradename to be included in the Subject Identity information.

3.2.2.3. Verification of Country

Google follows the CP when verifying the country associated with a Subject.

3.2.2.4. Authorization by Domain Name Registrant

Google follows the CP when verifying that the Applicant is the Domain Name Registrant or has control over the concerned FQDN.

The I&A procedures for Certificates that will include the domain name of a server include the following:

- Verify that the domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA). Subdomains must be for a domain appropriately registered with these organizations.
- Verify that the Domain registration information in the WHOIS database is public and shows the name, physical address, and administrative contact information for the entity to be named as the Subject in the Certificate. When a WHOIS database is not available, obtain compensating confirmation from the registry or registrar;
- Verify that the entity to be named as the Subject in the Certificate is the registered holder of the domain name, or alternatively, that it has the exclusive right to use the domain name by (i) verifying the identity of the person that is the registered holder of the domain name, and (ii) obtaining a verified confirmation from such owner of the domain name confirming such exclusive right to use the domain name;
- Verify that the entity to be named as the Subject in the Certificate is aware of its registration of the domain name.

Google may require additional proof of ownership from the Applicant in case of doubt.

3.2.2.5. Authentication for an IP Address

Google follows the CP when verifying that the Applicant has control over a concerned 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 - twenty-seven (27) months;
- Domain name - twenty-seven (27) months;
- Authority of Applicant - twenty-seven (27) months.

3.2.3. Authentication of individual identity

Google maintains procedures to ensure that its Identification and Authentication practices comply with the provisions on individual identification as set out in the CP.

3.2.4. Non-verified subscriber information

Google does not verify the following subscriber information:

- Organizational Unit (OU);
- Organization-specific information not used for identification purposes;
- Other information designated as non-verified in the certificate.

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. The verification is based on one or several of the sources listed in section 3.2.2 and its respective subsections.

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.

3.2.6. 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.

3.4. Identification and authentication for revocation request

Appropriate identification and authentication procedures are followed when evaluating requests for Certificate Revocation. If revokation is requested by the subscriber, identification and authentication is performed in accordance with section 3.2. For revokation requests made by the 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 a Google Certificate that names an entity as the Subject may be submitted by a Representative employed by or contracted by, and authorized to act on behalf of the concerned entity.

4.1.2. Enrollment process and responsibilities

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

- The identity of the Subscriber to be named as the Subject in the Certificate;
- The Public Key to be included in the Certificate (if the Subscriber has generated its own Key Pair);
- The fully qualified domain names to be included in the Certificate (if the Certificate will contain a domain name);
- An executed Subscriber Agreement, which may be electronic;
- Any other relevant information that Google requests.

4.2. Certificate application processing

Google performs the applicable I&A procedures and verifies the completeness accuracy and authenticity of the information provided by the Applicant prior to issuing a Google Certificate. This includes:

- Verifying that the Applicant has provided a well-formed, valid CSR, containing a valid signature;
- Obtaining a Public Key from the Applicant or, optionally, generating an asymmetric Key Pair on its behalf.
- Verifying that identifying data provided by the Applicant is valid.
- Verifying that the identifying data pertains to the Applicant and/or the Subject of the Certificate, as applicable.
- Verifying that the Applicant is permitted to obtain a Certificate under the relevant stipulations of the Google CP and this CPS.

4.2.1. Performing identification and authentication functions

Google performs identification and authentication of all required Subscriber information, as specified in section 3.2. If this information is not included in the certificate application and cannot be readily obtained from a trusted internal data source, the employee who processes the application requests 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 may approve an application if all required subscriber information has been provided and validated. All other request 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. Certification Authority Authorization (CAA) records

Google does not review Certificate Authority Authorization (CAA) DNS Resource Records for certificate application processing.

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.

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 e-mail 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 Subject 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

No stipulation.

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 matter, 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

Not applicable.

4.6.3. Processing certificate renewal requests

Not applicable.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6. Publication of the renewal certificate by the CA

Not applicable.

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

Not applicable.

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 certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

4.8.1. Circumstance for certificate modification

Not applicable.

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 is generated.

4.9.1. Circumstances for revocation

Certificates that have expired are not revoked.

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 the Google revoke 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 no longer complies with the requirements of Appendix A;
4. Google obtains evidence that the Certificate was misused;
5. Google is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
6. Google is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP 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);
7. Google is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
8. Google is made aware of a material change in the information contained in the Certificate;
9. Google is made aware that the Certificate was not issued in accordance with the Requirements applicable under the CP and this CPS;
10. Google determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. Google for any reason ceases operation of the CA that has issued the concerned Certificate and has not made arrangements for another CA to provide revocation support for the Certificate;

12. Google's right to issue Certificates expires or is revoked or terminated, unless it has made arrangements to continue maintaining the CRL/OCSP Repository;
13. Google is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
14. Revocation is required by the CP and/or Certification Practice Statement; or
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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 the Issuing CA 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 Appendix A,
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 the applicable Certification Practice Statement;
6. Google determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Google or the Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. Google or Subordinate CA's right to issue Certificates expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the CP and/or this CPS; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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, inappropriare conduct and other certificate related matters can be submitted via e-mail to contact@pki.goog. If the request or report is related to a potential compromise of the private key of a certificate, the requestor 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

The evaluation of a Certificate revocation request begins within 24 hours after the request has been received. If Google determines that a Revocation is warranted it updates the CRL promptly and in no case later than one business day following Revocation.

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 CRLs, that CRLs is updates and reissues 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)

Google maintains sufficient resources to provide a response time for CRL and OCSP responses of ten seconds or less under normal operating conditions.

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 RFC2560 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 RFC2560.

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 Subscriber Certificates, OCSP data is updated at least every three days. It has a mimumum validity of one day and a maximum validity time of seven days.

For Subordinate CA Certificates, OCSP data is updated at least every twelve (12) months and 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 re key compromise

In the case of a compromise of the private key used to sign certificates, Subscriber must immediately notify Google that the Subscriber's certificate has been compromised. Google will revoke the concerned signing key, and publish a CRL to make relying parties aware that the certificates issued off the signing key can no longer be trusted.

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

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

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

Not applicable.

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 exprires 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 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.

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 equipped with uninterruptable power supply and air conditioning to ensure reliable operations.

5.1.4. Water exposures

No stipulation.

5.1.5. Fire prevention and protection

No stipulation.

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 a backup facility for its CA infrastructure which also holds copies of the CA private keys for redundancy. The backup facility has 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.

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.

5.2.2. Number of persons required per task

The Private Key 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

No stipulation.

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 enforces appropriate personnel and management policies which are sufficient to provide reasonable assurance that its personnel are competent and that they perform their duties in a manner that is satisfactory and in accordance with this CPS.

All personnel operating the Google CAs are Google employees. Contractors or other third parties will not be allowed to act in Trusted Roles maintaining a Google CA.

5.3.2. Background check procedures

Google follows a set of established procedures for selecting and evaluating personnell 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 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. Independent contractors will not be used in Trusted Roles.

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 and 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 any audit logs generated for at least seven years, or longer if required by law and makes these audit logs 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

No stipulation.

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

Google's security program comprises an annual 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 cause 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.

Google follows a formal documented vulnerability correction process that includes 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 on at least an annual basis and after infrastructure modifications that it determines are significant.

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

A backup of archive information is maintained at a distinct, separate location with similar security and availability requirements.

5.5.4. Archive backup procedures

Backup and recovery procedures exist and can be utilized so that a complete set of backup copies will be available in the event of the loss or destruction of the primary archives.

5.5.5. Requirements for time-stamping of records

All archived records will be time-stamped by the CA's normal logging facilities. Such time information 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

If a disaster causes a Google CA to become inoperative, Google will re-initiate its operations on replacement hardware at a comparable, secured facility after ensuring the integrity and security of the CA systems.

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 the 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 the 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 taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing an affected facility following a disaster and prior to restoring a secure environment either at the original or a remote site.

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

Google maintains a backup site in a remote location that mirrors its primary facility, so that if any software or data is corrupted it can be restored from the backup site via a secure connection.

Backups of all relevant software and data are taken 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 posesses appropriate disaster recovery capabiliities, 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.

Subscriber Key Pairs are generated (i) by the Subscriber by software supplied by their device or operating system, (ii) by by a Google Service, or (iii) by an authorized member of Google's Information Security Team.

Key pairs for intermediate CAs are generated in accordance with the requirements set forth by the corresponding root CA including any contractual obligations that might exist between Google and the root CA.

6.1.2. Private key delivery to subscriber

If applicable, Private Keys are delivered to Subscribers in a secure manner in accordance with applicable Google policy on transferring confidential information. Subscriber Private Keys are encrypted for transport to the 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 Secure Sockets Layer (SSL).

6.1.4. CA public key delivery to relying parties

The public keys of Google CAs are made available from the online repository at http://pki.goog/. 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.

6.1.6. Public key parameters generation and quality checking

For RSA keys, Google confirms that the value of the public exponent is an odd number equal to 3 or more.

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 in the following cases:

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 and 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 Certificate Authority Key Pairs are generated in pre-planned key generation ceremonies. Upon finalization of the ceremony, all individuals involved sign off on the successful completion of the script, and thoroughly describe any exceptions that may have been applied in the process.

Records are maintained at least for the lifetime of the key pair.

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 and comprises technical, organizational, and procedural measures.

6.6.3. Life cycle security controls

System security management is controlled through the privileges assigned to the operating system accounts of the CA infrastructure and by the Trusted Roles described in this CPS.

6.7. Network security controls

The servers of Google CAs are located behind hardware firewall devices that restrict access to only the internal Google network, and only to ports used for managing the CA and issuing Certificates.

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 standards.

In cases where stipulations of RFC 5280 and the applicable CA/Browser Forum Baseline Requirements differ, the Baseline Requirements notion will be adhered to.

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 Google Certificate Profiles appendix.

7.1.3. Algorithm object identifiers

See Google Certificate Profiles appendix.

7.1.4. Name forms

By issuing a Certificate, Google represents that it followed the procedure set forth in this CPS to verify that, as of the issuance date, all of the Subject Information was accurate. Google does not include a Domain Name in a Subject attribute except as specified in Section 3.2.5.1

Wildcard names may be used for wildcard certificates.

Google does not issue Certificates containing IP Addresses or Internal Names in the Subject Information.

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.

SSL certificates may not contain 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.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy object identifier

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

- CA/Browser Forum Baseline Requirements: 1.3.6.1.4.1.11129.2.5.1
- Domain Validated (DV) Certificates 2.23.140.1.2.1
- Organization Validated (OV) Certificates 2.23.140.1.2.2
- Extended Validation (EV) 2.23.140.1.1
- Individual Validated (IV) 2.23.140.1.2.3
- EV Code Signing 2.23.140.1.3
- Non-EV Code Signing 2.23.140.1.4

7.1.7. Usage of Policy Constraints extension

The PolicyConstraints extension shall be empty.

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

No stipulation.

7.3. OCSP profile

All Google CAs support OCSP, and its responders conform to the RFC 2560 standard. The OCSP responder within the AuthorityInformationAccess (AIA) extension is identified via an OCSP responder URL.

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

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 and audit that addresses the criteria specified in the WebTrust standard;
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 licensed by WebTrust;
5. 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 cover a validation of controls relevant for the proper operation of the CAs. In particular they cover an assessment of the auditee's compliance with the WebTrust Principles and Criteria for Certification Authorities formulated by CPA Canada and the American Institute of Certified Public Accountants (AICPA) as well as the CA/Browser Forum's Baseline Requirements.

8.5. Actions taken as a result of deficiency

Significant deficiencies identified during a Compliance Audit will result in a determination of actions to be taken by the CA managament. These decisions are made with input from the auditor, and implemented 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 the Qualified Auditor.

The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates by the Google CAs.

8.7. Self-Audits

Google monitors its adherance 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 will never 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 is 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 Baseline ("CABF") requirements. 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 LIABILE 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

9.9.1. By subscriber

No stipulation.

9.9.2. By relying parties

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 and Acronyms

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").

Applicant: An individual or Legal Entity that requests the issuance, renewal, re-key, or revocation of a Google Certificate on behalf of an entity or where authorized, on behalf of himself or herself.

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

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): Generally, an organization that is responsible for the creation, issuance and management of certificates. In the Google PKI, Google is the Certification Authority. 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.

Certification Practice Statement (CPS): This document.

Certificate Policy (CP): Google's Certificate Policy

Certificate Revocation List (CRL): A regularly updated list of revoked Certificates that is created and digitally signed by the CA that originally issued the Certificates listed in such CRL.

CN: Common Name

DBA: Doing Business As

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.

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).

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.

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

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.

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 must be kept secret by the holder of the Key Pair, and that is used to generate digital signatures and/or to decrypt electronic records that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that is intended to be publicly shared with recipients of digitally signed electronic records and that is used by such recipients to verify Digital Signatures created with the corresponding Private Key and/or to encrypt electronic records so that they can be decrypted only with the 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): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). A role within the Google PKI that administers the Registration Process and processes requests for Certificate Reissuance and Revocation.

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.

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.

Subject: The individual or organization named in a Certificate's "Subject" field.

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.

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.

Appendix B: Permissible Cryptographic Algorithms and Key Sizes

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

Type	Permissible values
Digest Algorithm	SHA1 (allowed if issued before 2015-12-31), SHA-256, SHA-384 or SHA-512
RSA	2048 or longer
ECC	NIST P-256, P-384, or P-521

For RSA keys the public exponent must be an odd number equal to 3 or more.

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).

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
- Code Signing EKU=1.3.6.1.5.5.7.3.3
- Time stamping EKU=1.3.6.1.5.5.7.3.8

Certificates, do not combine server authentication with code signing uses unless the uses are separated by application of Extended Key Uses ("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. Google may continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017.

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 maket of the respective CA.
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey RFC 5280
extension:basicConstraints	marked critical, cA is TRUE
extension:keyUsage	digitalSignature, keyCertsign and cRLSign are set, other bits are not set

Subordinate 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
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:keyUsage	not marked critical, digitalSignature, keyCertsign, and cRLSign bits are set, all other bits are not set
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Standard Validation Client Certificates

Field	Content
validity:not after	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
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	is either absent or is empty
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the 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:keyUsage	not marked critical, bit positions digitalSignature bit must be set, keyExchange may be set, other bits must not be set
extension:extkeyUsage	not marked critical, id-kp-clientAuth RFC 5280, id-kp-emailProtection RFC 5280, or szOID_KP_DOCUMENT_SIGNING MS OID may be present. Other values should not be present.

Standard Code Signing Certificates

Field	Content
validity:not after	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	Contains countryName, organizationName and commonName
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 is empty
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the 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:keyUsage	not marked critical, digitalSignature bit must be set, other bits must not be set
extension:extkeyUsage	not marked critical, must include codeSigning. Other values must not be present.

Standard Validation TLS Certificates

Field	Content
validity:not after	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	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 is empty
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the issuing CA's OCSP responder

Field	Content
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
extension:keyUsage	not marked critical, digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extkeyUsage	not marked critical, must include serverAuth, may include clientAuth RFC 5280

Organization Validation TLS Certificates

Field	Content
validity:not after	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	Contains countryName, locality, organizationName and 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 maked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or is empty
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the 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

Field	Content
extension:keyUsage (optional)	not marked critical, digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extkeyUsage	not marked critical, must include serverAuth, may include clientAuth 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