Amazon Trust Services Certification Practice Statement

Version 1.0.5

1. INTRODUCTION

1.1 Overview

Amazon Trust Services ("Amazon") has established the Amazon Public Internet Public Key Infrastructure ("Amazon PKI"). This CPS outlines the principles and practices related to the Amazon PKI certificate issuance services and describes the practices used to comply with the Amazon CP and other applicable policies.

This practice statement is designed to be read in conjunction with the Amazon Certificate Policy. All defined terms and acronyms in the CP have the same definitions in this document unless redefined in §1.6 of this document.

The Amazon PKI conforms to the current version of the guidelines adopted by the Certification Authority/ Browser Forum ("CAB Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates ("Baseline Requirements"), the Guidelines for Extended Validation Certificates ("EV Guidelines") and the Guidelines for Extended Validation Code Signing ("EV Code Signing Guidelines), each of which are published at https://www.cabforum.org. If any inconsistency exists between this CPS and the Baseline Requirements, the EV Guidelines, or EV Code Signing Guidelines then the associated requirement or guideline document shall take precedence.

This CPS is only one of several documents that control Amazon PKI certification services. Other important documents include both private and public documents, such as the CP, Amazon's agreements with its customers, and Amazon's privacy policy. Amazon may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties. The document name, location of, and status, whether public or confidential, are detailed below. This is not an exhaustive list.

Document	**Status**	**Location**
Amazon Certificate Policy	Public	Amazon Repository
Amazon Certification Practice Statement	Public	Amazon Repository
Subscriber Agreement	Public	Amazon Repository
Terms of Use	Public	Amazon Repository
Amazon Privacy Policy	Public	https://www.amazon.com/gp/help/customer/display.html?nodeId=468496
CA Procedure Documents	Confidential	Presented to auditors accordingly

This CPS, related agreements, and Certificate policies referenced within this document are available online at https://www.amazontrust.com/repository.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine primary components that cover the security controls and practices and procedures for certificate issuance services within the Amazon PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement “Not applicable” or “No stipulation.”

This document is the CPS for the following Certification Authorities:

CA Type	CA Distinguished Name	Key pair type and parameters	SHA-256 Key Fingerprint	Validity Period
Root CA	C=US O=Amazon CN=Amazon Root CA 1	RSA, n has 2048-bits e=65537	fbe3018031f9586b cbf41727e417b7d1 c45c2f47f93be372 a17b96b50757d5a2	2015-05-26 00:00:00 GMT to 2038-01-17 00:00:00 GMT
Root CA	C=US O=Amazon CN=Amazon Root CA 2	RSA, n has 4096-bits e=65537	7f4296fc5b6a4e3b 35d3c369623e364a b1af381d8fa71215 33c9d6c633ea2461	2015-05-26 00:00:00 GMT to 2040-05-26 00:00:00 GMT
Root CA	C=US O=Amazon CN=Amazon Root CA 3	EC, NIST P-256 curve	36abc32656acfc64 5c61b71613c4bf21 c787f5cabbee4834 8d58597803d7abc9	2015-05-26 00:00:00 GMT to 2040-05-26 00:00:00 GMT
Root CA	C=US O=Amazon CN=Amazon Root CA 4	EC, NIST P-384 curve	f7ecded5c66047d2 8ed6466b543c40e0 743abe81d109254d cf845d4c2c7853c5	2015-05-26 00:00:00 GMT to 2040-05-26 00:00:00 GMT
Root CA	C=US ST=Arizona L=Scottsdale O=Starfield Technologies, Inc. CN=Starfield Services Root Certificate Authority - G2	RSA, n has 2048-bits e=65537	28689b30e4c306aa b53b027b29e36ad6 dd1dcf4b95399448 2ca84bdc1ecac996	2009-09-01 00:00:00 GMT to 2037-12-31 23:59:59 GMT

Effective June 10, 2015, the *Starfield Services Root Certificate Authority - G2* certification authority operates under this CPS. Prior to such date, the *Starfield Services Root Certificate Authority - G2* certification authority was operated under the Starfield Technologies, LLC Certificate Policy and Certification Practice Statement.

1.2 Document name and identification

This document is the Amazon Certification Practices Statement and was approved for publication by the APPMA. The following revisions were made to the original document:

Date	Changes	Version
2015-05-26	Initial release.	1.0.1

2015-06-10	Added new root.	1.0.2
2015-10-21	Updated to Amazon Trust Services and to use standard policy identifiers.	1.0.3
2015-12-08	Updated validation processes for wildcard DNs, email addresses, and Subordinate CAs.	1.0.4
2017-01-12	Yearly update	1.0.5

The OID for this CPS is 1.3.187.129.2 {iso(1) identified-organization(3) amazon(187) documents(129) cps(2)} Subsequent revisions to this CPS may have new OID assignments.

1.3 PKI participants

1.3.1 Certification authorities

Amazon is a CA that issues digital certificates. As a CA, Amazon performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about Amazon products and services is available at www.amazon.com.

CAs issue certificates in accordance with the Amazon CP. Subscriber certificates are only issued from Root CAs as necessary to meet the User Agent Verification Requirements of Appendix C of the Baseline Requirements and may only be issued to Amazon Trust Services or an affiliated company. Amazon Trust Services or an affiliated company must have the right to use or legitimate control of all domain names and IP addresses in such subscriber certificates.

1.3.2 Registration authorities

Amazon may delegate the performance of certain functions to an RA and/or other third parties (each a "Delegated Third Party") to request certificates and/or perform identification and authentication for end user certificates. The specific role of an RA or Delegated Third Party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs operate identity management systems and may manage the certificate lifecycle for end users. Amazon contractually obligates each Delegated Third Party to abide by the policies and industry standards that are applicable to that Delegated Third Party's role in certificate issuance, management, revocation or other related task that the Delegated Third Party performs.

RA personnel involved in the issuance of publicly trusted SSL Certificates must undergo training as specified in 5.3.3 Training Requirements set forth in Section 5.3.3 hereof. An RA or identity management system supporting a particular community of interest with custom identity vetting practices that differ from those found herein may submit documentation to the APPMA for review and approval. The documentation must contain sufficient detail to ensure that all tasks required by the CP will be performed.

1.3.3 Subscribers

Subscribers use the Amazon PKI to support transactions and communications. Subscribers are not always the party identified in a certificate, such as when certificates are issued to an organization's employees or when the subject owner has granted control of the subject to the subscriber. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant.

1.3.4 Relying parties

Relying Parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate. The location of the CRL distribution point and OCSP responder is detailed within the certificate.

1.3.5 Other participants

Other participants include Accreditation Authorities (such as Policy Management Authorities, Federation Operators, Application Software Vendors, and applicable Community of Interest sponsors); Bridge CAs and CAs that cross certify Amazon CAs as trust anchors in other PKI communities, CMAs, RSPs, CSAs and TSAs.

If the CA subcontracts CMA, RSP, CSA, TSA, or other functions, the CA ensures that compliance with the CP is required in the agreement with the subcontractor. The CA may use a practices statement of the subcontractor as evidence of compliance if, and only if, the subcontractor's practices are audited by an independent external auditor on at least an annual basis and the subcontractor submits the results of each audit to the CA.

1.4 Certificate usage

A digital certificate (or certificate) is formatted data that cryptographically binds an identified Subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate. However, the sensitivity of the information processed or protected by a certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CPS.

1.4.2 Prohibited certificate uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the certificate was verified as reasonably correct when the certificate issued.

Certificates issued under this CPS may not be used (i) 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; or (ii) where prohibited by law.

Additionally, Certificates issued under this CPS may not be used for "traffic management" or man-in-the-middle purposes.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS and the documents referenced herein are maintained by the APPMA, which can be contacted at:

```
Amazon PKI Policy Management Authority
410 Terry Ave. North
Seattle, WA, 98109-5210
+1 206 266 1000
Web: www.amazon.com
Email: appma@amazon.com
```

1.5.2 Contact person

```
Attn: Amazon Trust Services Legal Department
Amazon PKI Policy Management Authority
410 Terry Ave. North Seattle, WA, 98109-5210
+1 206 266 1000
Web: www.amazon.com
Email: appma@amazon.com
```

1.5.3 Person determining CPS suitability for the policy

The APPMA determines the suitability and applicability of this CPS based on the results and recommendations received from an independent auditor. The APPMA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4 CPS approval procedures

The APPMA approves the CPS and any amendments. Amendments are made after the APPMA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by publishing an addendum. The APPMA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change.

1.6 Definitions and acronyms

1.6.1 Definitions

Affiliated Organization
: An organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate.

Applicant
: An entity applying for a certificate.

Application Software Vendor
: A software developer whose software displays or uses Amazon certificates and distributes Amazon root certificates.

Base Domain

A Domain Name which is formed by pruning one or more labels from the left side of a FQDN. Base Domains do not include public suffixes or any Domain Name which is created by removing one or more labels from the left side of a public suffix.

CA/Browser Forum

A group made up of Certificate Authorities and Browsers that establish and manage the requirements all public Certificate Authorities must meet.

Certificate Transparency

An open framework for monitoring and auditing digital certificates.

Crypto-module

A hardware device such as a smartcard, token or hardware security module that generates and manages cryptographic keys securely.

Entropy

The randomness collected by a system for use in cryptography or other uses that require random data.

Key Pair

A Private Key and associated Public Key.

OCSP Responder

An online software application operated under the authority of Amazon and connected to its repository for processing certificate status requests.

Private Key

The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key

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

Punycode

Punycode is a way to represent Unicode with the limited character subset of ASCII supported by the Domain Name System.

RA Practices Statement

A statement of the practices, which an RA follows.

Relying Party

An entity that relies upon either the information contained within a certificate or a time stamp token.

Subject

The entity named in the certificate.

Subscriber

As applicable, the entity identified as the Subject in the certificate and/or the entity that contracted with Amazon for the certificate's issuance.

Subscriber Agreement

An agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

Trusted Agent

An accountant, lawyer, notary, postal carrier or any entity certified by a State or National Government as authorized to confirm identities or other reliable third party.

WebTrust

The current version of the AICPA/CICA WebTrust Program for Certification Authorities.

X.509
: The ITU-T standard for Certificates and their corresponding authentication framework

1.6.2 Acronyms

APPMA
: Amazon PKI Policy Management Authority

CA
: Certificate Authority or Certification Authority

CAB
: "CA/Browser" as in "CAB Forum"

CMA
: Certificate Manufacturing Authority

CP
: Certificate Policy

CPS
: Certification Practice Statement

CRL
: Certificate Revocation List

CSA
: Certificate Status Authority

CSR
: Certificate Signing Request

ETSI
: European Telecommunications Standards Institute.

EV
: Extended Validation

FIPS
: (US Government) Federal Information Processing Standard

FQDN
: Fully Qualified Domain Name

FTP
: File Transfer Protocol

HSM
: Hardware Security Module

HTTP
: Hypertext Transfer Protocol

IANA
: Internet Assigned Numbers Authority

ICANN
: Internet Corporation for Assigned Names and Numbers

IdM
: Identity Management System

IDN
: Internationalized Domain Name

IETF
: Internet Engineering Task Force

ITU
: International Telecommunication Union

ITU-T
: ITU Telecommunication Standardization Sector

NIST
: National Institute of Standards

OCSP
: Online Certificate Status Protocol

OID
: Object Identifier

PKCS
: Public Key Cryptography Standard

PKI
: Public Key Infrastructure

PKIX
: IETF Working Group on Public Key Infrastructure

RA
: Registration Authority

RFC
: Request for Comments (at IETF.org)

RSP
: Repository Service Provider

SHA
: Secure Hashing Algorithm

SSL
: Secure Sockets Layer

TLD
: Top Level Domain

TLS
: Transport Layer Security

TSA
: Time-stamp authority

TSP
: Time-stamp policy

TST
: Time-stamp token

URL
: Uniform Resource Locator

UTC
: Coordinated Universal Time

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Amazon makes its root certificates, revocation data for issued digital certificates, CPs, CPSs, and standard Subscriber Agreements available in public repositories. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this CPS. Amazon's legal

repository is located at https://www.amazontrust.com/repository. Amazon publicly trusted root certificates and its CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems that are designed to minimize downtime.

Amazon publishes all Subordinate CA Certificates which are not Technically Constrained Subordinate CA Certificate and all Cross Certificates it issues. For each such certificate, Amazon includes the certificate, a link to CPS for the subject of the certificate, and a link to the public attestation of operations of the CA in the Amazon repository located at https://www.amazontrust.com/repository.

2.2 Publication of certification information

The Amazon certificate services and the repository are on the web at https://www.amazontrust.com/repository (and via URIs included in the certificates themselves).

Links to test Web Pages demonstrating valid, revoked, and expired certificates are included in the repository.

2.3 Time or frequency of publication

CA certificates are published in a repository as soon as possible after issuance. CRLs are published in accordance with §4.9.7

Amazon may publish new CRLs prior to the scheduled issuance of the next CRL. New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party representations and warranties (as described in §9.6.4) are typically published within seven days after their approval.

2.4 Access controls on repositories

Read only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Certificates are issued with distinguished names and subject alternative names that comply with the CP.

3.1.2 Need for names to be meaningful

Amazon uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the certificate and the entity that is the issuer of the certificate.

3.1.3 Anonymity or pseudonymity of subscribers

The subscriber is not identified in certificates that do not contain organizationName, surname, or givenName. Relying parties should treat the subscriber as anonymous.

3.1.4 Rules for interpreting various name forms

Distinguished Names in certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in certificates are interpreted as Uniform Resource Identifiers and HTTP references.

Certificates do not assert any specific relationship between the subscriber and registrant(s) of DNS name(s) contained in certificates.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

Subscribers may not request certificates with content that infringes on the intellectual property rights of another entity. Unless otherwise specifically stated in this CPS, Amazon does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. Amazon may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2 Initial identity validation

Amazon may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. Amazon may refuse to issue a Certificate at its sole discretion.

3.2.1 Method to prove possession of private key

Amazon verifies a digital signature on a signed object containing the matching public key to confirm possession of the private key. The signed object is normally a PKCS#10 certification request, but may be in other formats.

3.2.2 Authentication of organization identity

Amazon follows the Amazon CP for authentication of organization identification.

Amazon uses the following methods to confirm that the Applicant has control of or right to use Domain Names:

1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; or
2. Confirming authorization of the Certificate's issuance directly with the Domain Name Registrant using a Reliable Method of Communication verified by either (i) communication with the Domain Name Registrar or (ii) being listed as the contact information for "registrant", "technical", or "administrative" contacts listed in the WHOIS record for the Base Domain; or
3. Confirming authorization for the Certificate's issuance through an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; or

4. Relying upon a Domain Authorization Document that meets the requirements listed below; or
5. Having the Applicant demonstrate control over the FQDN or Base Domain by making an agreed-upon change to information found to a file hosted in the "/.well-known/cabforum" directory at either the FQDN or the Base Domain in accordance with RFC 5785; or
6. Having the Applicant demonstrate control over the FQDN or Base Domain by the Applicant making a change to information in a DNS TXT record for the FQDN or Base Domain where the change is a random number with at least 128 bits of entropy provided to the Applicant by the CA; or
7. Having the Applicant demonstrate control over a FQDN by making an agreed upon change to DNS records for a Domain Name which is formed by pruning zero or more labels from the left side of the requested FQDN or formed by prepending a label to the left side of the requested FQDN where an appended label exhibits at least 128 bits of entropy and is provided to the Applicant by the CA; or
8. Having the Applicant demonstrate control over the requested FQDN by the CA confirming, in accordance with section 11.1.1, the Applicant's controls the FQDN (or Base Domain of the FQDN) returned from a DNS lookup for CNAME records for the requested FQDN; or
9. Having the Applicant demonstrate control over the requested FQDN by the CA confirming, in accordance with section 11.1.2, that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the requested FQDN; or
10. Having the Applicant demonstrate practical control over the FQDN by providing a TLS service on a host found in DNS for the FQDN and having the CA (i) initiate a TLS connection with the host and (ii) verify a response specified by the CA that exhibits 128 bits of entropy and is a in a format recognized as a valid TLS response.

Amazon does not use methods 9, 10, or 11 for validating wildcard names.

Amazon uses the following methods to confirm the Applicant has control of or right to use Email Addresses:

1. Confirming authorization of the Certificate's issuance by contacting the requested email address, or
2. Confirming control of the FQDN in the Domain portion of the Email address using methods 1, 2, 5, 7, or 8 above.

3.2.3 Authentication of individual identity

Amazon follows the Amazon CP for authentication of individual identification.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Amazon follows the Amazon CP for validation of authority.

Amazon allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then Amazon will not accept any certificate requests that are outside this specification. A request to limit authorized individuals is not effective until approved by Amazon. Amazon will provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for interoperation

Amazon discloses cross certificates by placing copies of the cross certificate in the Repository.

3.3 Identification and authentication for re-key requests

Amazon does not rekey certificates without following the same procedures as issuing a new certificate.

3.3.1 Identification and authentication for routine re-key

As per §3.2.

3.3.2 Identification and authentication for re-key after revocation

As per §3.2.

3.4 Identification and authentication for revocation request

Amazon or an RA authenticates all revocation requests that are at the Subscriber's request. Amazon may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

When the revocation is at the CA's request, such as for cause in accordance with §4.9, 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

The CA follows the Amazon CP to determine who can submit a certificate application.

4.1.2 Enrollment process and responsibilities

In no particular order, the enrollment process includes:

- Submitting a certificate application,
- Generating a key pair,
- Delivering the public key of the key pair to Amazon,
- Agreeing to the applicable Subscriber Agreement, and,

- Paying any applicable fees.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Amazon or an RA (as described in §1.3.2) verifies the application information and other information specified in the Amazon CP. As part of this verification, Amazon checks the certificate against an internal database of previously revoked certificates and rejected certificate requests to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, an Amazon employee, RA, or agent skilled in the language assists in the identification and authentication.

Amazon Root CAs do not check CAA records prior to issuing certificates.

4.2.2 Approval or rejection of certificate applications

Amazon follows the Amazon CP with respect to new gTLDs.

For Applications for a Subordinate CA where the Subordinate CA will not be controlled by Amazon, Amazon ensures that all the following are true:

- The APPMA has approved the Subordinate CA
- There is a contract in place requiring the Subordinate CA to comply with CA/Browser Forum guidelines
- The CA generated and stores its keys on a HSM that meets the requirements in the CP
- The CA had the key generation audited by a qualified auditor. This is not required to be a WebTrust licensed auditor, but the auditor must meet items 1, 3, 6, and 7 of section 8.2 of the CP.
- If the Subordinate CA certificate is not technically constrained, then the contract requires the Subordinate CA operator to provide evidence of a WebTrust audit with a period ending not more than one year prior to application or a WebTrust point in time readiness assessment that occurred no more than one year prior to application. Additionally, the CA must have WebTrust audits covering periods no longer than one year in duration where each audit period must immediately start after the previous period end with no gaps.

Amazon will post links to Subordinate CA certificates, CP, CPS, and audit options (if applicable) in its repository.

4.2.3 Time to process certificate applications

The time required to process a certificate application shall not exceed the time to approve or reject the application.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Amazon confirms the source of a certificate request before issuance. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the certificate is stored in a database and sent to the Subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Amazon will deliver certificates within a reasonable time after issuance. Generally, Amazon delivers certificates via email to the email address designated by the Subscriber, via a programmatic method such as an API, or via download from a website.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Subscribers are solely responsible for installing the issued certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted on the earlier of

- The Subscriber's use of the certificate,
- 30 days after the certificate's issuance.

4.4.2 Publication of the certificate by the CA

Amazon publishes all CA certificates in its repository and publishes end entity certificates by delivering them to the Subscriber using email or an API.

Subordinate CA certificates are provided to relevant entities as part of the certificate chain.

4.4.3 Notification of certificate issuance by the CA to other entities

RAs may receive notification of a certificate's issuance if the RA was involved in the issuance process.

Amazon may notify the public of the issuance of a certificate by adding it to one or more publicly accessible Certificate Transparency (CT) Logs.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use Certificates in accordance with their intended purpose.

4.5.2 Relying party public key and certificate usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. Amazon does not warrant that any third party software will support or enforce the controls and requirements found herein.

A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of loss prior to relying on a certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate. Any warranties provided by Amazon are only valid if a Relying Party's reliance was reasonable.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. The digital signature or SSL/TLS session was created during the operational period of a valid certificate and can be verified by referencing a valid certificate,
2. The certificate is not revoked and the Relying Party checked the revocation status of the certificate prior to the certificate's use by referring to the relevant CRLs or OCSP responses, and
3. The certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time stamp token, a Relying Party must:

1. Verify that the time stamp token has been correctly signed and that the Private Key used to sign the time stamp token has not been compromised prior to the time of the verification,
2. Take into account any limitations on the usage of the time stamp token indicated by the time stamp policy, and
3. Take into account any other precautions prescribed in this CPS or elsewhere.

4.6 Certificate renewal

Amazon treats all certificate renewal requests as applications for certificate issuance and follows the same procedures used when issuing a certificate.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

See §4.1.1.

4.6.3 Processing certificate renewal requests

See §4.2.

4.6.4 Notification of new certificate issuance to subscriber

See §4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See §4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See §4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See §4.4.3.

4.7 Certificate re-key

Amazon treats all certificate re-key requests as applications for certificate issuance and follows the same procedures used when issuing a certificate.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

See §4.1.1.

4.7.3 Processing certificate re-keying requests

See §4.2.

4.7.4 Notification of new certificate issuance to subscriber

See §4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See §4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See §4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See §4.4.3.

4.8 Certificate modification

Amazon treats all certificate modification requests as applications for certificate issuance and follows the same procedures used when issuing a certificate.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

See §4.1.1.

4.8.3 Processing certificate modification requests

See §4.2.

4.8.4 Notification of new certificate issuance to subscriber

See §4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See §4.4.1.

4.8.6 Publication of the modified certificate by the CA

See §4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See §4.4.3.

4.9 Certificate revocation and suspension

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period.

4.9.1 Circumstances for revocation

Amazon will revoke a certificate if the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation.

Amazon will follow the Amazon CP and revoke a certificate in accordance with §4.9.1.1 and §4.9.1.2 of the Amazon CP.

Amazon always revokes a certificate if the binding between the Subject and the Subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

Amazon will revoke a cross certificate if the cross certified entity (including Amazon) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross certificate.

4.9.2 Who can request revocation

Any appropriately authorized party, such as a recognized representative of a Subscriber or cross-signed partner, may request revocation of a certificate. Amazon may revoke a certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, compromise, or non-compliance with the CP or CPS. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

Subscribers may request revocation of their own certificates by emailing aws-tsp-requests@amazon.com. All reports need to include sufficient detail to identify the specific certificates to be revoked.

4.9.3 Procedure for revocation request

Amazon processes a revocation request as follows:

1. Amazon logs the identity of entity making the request or problem report and the reason for requesting revocation. Amazon may also include its own reasons for revocation in the log.
2. Amazon may request confirmation of the revocation from a known administrator, where applicable, via out of band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, Amazon revokes the certificate.
4. For requests from third parties, Amazon personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:

    a. The nature of the alleged problem,
    b. The number of reports received about a particular certificate or website,
    c. The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. Relevant legislation.
5. If Amazon determines that revocation is appropriate; Amazon personnel revoke the certificate and update the CRL.

Amazon maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, Amazon forwards complaints to law enforcement.

Instructions for requesting revocation are linked from the Repository.

4.9.4 Revocation request grace period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. Amazon may grant and extend revocation grace period on a case-by-case basis.

4.9.5 Time within which CA must process the revocation request

Amazon will revoke a CA certificate within one hour after receiving clear instructions from the APPMA. Other certificates are revoked as quickly as practical after validating the revocation request, generally within the following time frames:

1. Certificate revocation requests for publicly trusted certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and

3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

4.9.6 Revocation checking requirement for relying parties

Prior to relying on information listed in a certificate, a Relying Party must confirm the validity of each certificate in the certificate path in accordance with IETF PKIX standards, including checking for certificate validity, issuer to subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each certificate in the chain.

4.9.7 CRL issuance frequency (if applicable)

Amazon will update and reissue CRLs with a frequency greater than or equal to that required by the Amazon CP.

4.9.8 Maximum latency for CRLs (if applicable)

CRLs for certificates issued to end entity Subscribers are posted automatically to the online repository within a commercially reasonable time after generation. Irregular, interim, or emergency CRLs are typically posted within four hours after generation and within 24 hours of determining of the occurrence of a key compromise. Regularly scheduled CRLs are posted prior to the next Update field in the previously issued CRL of the same scope.

OCSP responses are provided within a commercially reasonable time and no later than ten seconds after the request is received, under normal operating conditions. For EV certificates, responses are able to be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

4.9.9 On-line revocation/status checking availability

Amazon makes certificate status information available via OCSP for all certificates it issues.

4.9.10 On-line revocation checking requirements

A relying party must confirm the validity of a certificate prior to relying on the certificate.

Amazon OCSP responders comply with the requirements of the Amazon CP.

4.9.11 Other forms of revocation advertisements available

Amazon allows, but does not require, OCSP stapling.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

Amazon 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

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked certificate remains on the CRL until one additional CRL is published after the end of the certificate's validity period, except for revoked EV Code Signing Certificates, which remain on the CRL for at least 365 days following the certificate's validity period. OCSP information for Subscriber certificates is updated at least every four days. OCSP information for subordinate CA certificates is updated at least every 12 months and within 24 hours after revoking the certificate.

4.10.2 Service availability

Certificate status services are designed to be available 24x7.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

A Subscriber's subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12 Key escrow and recovery

Amazon 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. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

Certificate Manufacturing Facilities are located in the United States. Private keys for all CAs following this CPS are exclusively located in the United States unless otherwise stated in the Repository. Physical barriers, including solid walls that extend from real floor to real ceiling are in place to prevent unauthorized entry to Certificate Manufacturing Facilities.

5.1.2 Physical access

Physical access to Amazon PKI facilities is restricted to authorized Amazon employees, vendors, and contractors who require access to execute their jobs. Amazon uses multi-factor authentication mechanisms for access control as well as additional security mechanisms designed to ensure that only authorized individuals enter PKI facilities.

5.1.3 Power and air conditioning

Heating, ventilation, and air conditioning systems are designed to maintain environmental specifications provided system vendors.

5.1.4 Water exposures

Amazon's facilities are designed to protect CA systems from water exposure.

5.1.5 Fire prevention and protection

Amazon's facilities are designed to provide fire suppression for the CA.

5.1.6 Media storage

Amazon's facilities and processes are designed to protect media from accidental damage and authorized physical access.

5.1.7 Waste disposal

Storage media containing sensitive data is physically destroyed or securely overwritten prior to disposal or reuse. Printed documents containing sensitive data needing disposal are stored in locked shred bins which are periodically collected and destroyed by a data destruction company.

5.1.8 Off-site backup

Amazon maintains copies of CA private keys and activation data at multiple locations for redundancy. All copies are stored in a system or device validated as meeting FIPS 140 Level 3 to ensure that they are only accessible by trusted personnel.

5.2 Procedural controls

5.2.1 Trusted roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the Amazon PKI's operations. A list of personnel appointed to trusted roles is maintained and reviewed annually.

PKI Executive
: The Executive is responsible for overseeing all activities in the Amazon PKI, including appointment of persons to all other roles. The PKI Executive is a member of the PKI Policy Management Authority but cannot function in any other Trusted Role.

PKI Policy Management Authority Member
: The APPMA is responsible for approving this CPS and certain other documents related to CAs in the Amazon PKI. The APPMA approves the generation, revocation and suspension of CA certificates. APPMA members cannot serve in any other Trusted Role (except for PKI Executive).

PKI Managers
: Amazon PKI Managers are responsible for PKI Operations and CA documents, including the Certificate Policy, Certification Practice Statement, and this document. The PKI Manager cannot serve as a PKI Security Officer.

PKI Security Officer
: PKI Security Officers have a combination to the safe and/or PINs for the PED keys necessary to use the HSMs.

PKI Engineers
: PKI Engineers are responsible for CA systems development and operations.

Validation Specialists
: Validation Specialists are responsible for the collection and review of information in support of a certificate application. Validation Specialists look for discrepancies or other details requiring further explanation in the application and supporting information.

Internal Auditor
: Internal Auditors are responsible for overseeing internal compliance to determine if Amazon, an Issuer CA, or RA is operating in accordance with this CPS or an RA Practices Statement. This may include acting as Witness to ceremonies or holding credential or key required to initiate a ceremony.

5.2.2 Number of persons required per task

Amazon ensures that at least three people are required for CA key generation, CA signing key activation, and CA private key backup.

5.2.3 Identification and authentication for each role

All personnel are required to authenticate themselves to CA and supporting systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4 Roles requiring separation of duties

The PKI Executive may not concurrently serve as Internal Auditor, PKI Engineer, or Validation Specialist. Persons serving as Internal Auditors may not hold any other trusted role. Persons serving as members of the PMA may not serve as PKI Engineer or Validation Specialist.

For the issuance of Extended Validation certificates, the same person may not serve as both System Operator and Verification Operator.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The APPMA is responsible and accountable for Amazon PKI operations and ensures compliance with this CPS and the CP. Amazon personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties.

Management and operational support personnel involved in time stamp operations possess experience with information security and risk assessment and knowledge of time stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The APPMA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background check procedures

Amazon verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. Amazon requires each individual to appear in person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I 9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Background checks are refreshed at least every ten years.

5.3.3 Training requirements

Amazon provides suitable training to all staff before they take on a Trusted Role should they not already have the complete skill-set required for that role.

Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached.

Validation Specialists are trained in Amazon's validation and verification policies and procedures.

5.3.4 Retraining frequency and requirements

Personnel in Trusted Roles have additional training when changes in industry standards or changes in Amazon's operations require it.

Amazon provides refresher training and informational updates sufficient to ensure that Trusted Personnel retain the requisite degree of expertise.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Amazon employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7 Independent contractor requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles as specified in 5.3 Personnel controls and are subject to sanctions specified in 5.3.6 Sanctions for Unauthorized Actions.

5.3.8 Documentation supplied to personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP, this CPS, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of Amazon CA operations.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Audit log files are be generated for all events relating to the security and services of the CA. Where possible, the security audit logs are be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism are be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Amazon ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- the type of event;
- the date and time the event occurred;

- success or failure where appropriate;
- the identity of the entity and/or operator that caused the event;
- the identity to which the event was targeted; and
- the cause of the event.

5.4.2 Frequency of processing log

Logs are archived by the system administrator within 7 days of event activity. CA management reviews logs in the audit log repository at least every 93 days.

5.4.3 Retention period for audit log

Audit logs are retained for at least seven years and will be made available to the Amazon external independent auditor upon request.

5.4.4 Protection of audit log

Production and archived logical and physical audit logs are protected using a combination of physical and logical access controls.

5.4.5 Audit log backup procedures

Amazon makes regular backup copies of audit logs and audit log summaries and sends a copy of the audit log off-site on a monthly basis.

5.4.6 Audit collection system (internal vs. external)

Automatic audit data is generated and recorded at the application, network, and operating system level. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, Amazon Administrators will consider suspending its operation until the problem is remedied. Manually generated audit data is recorded by authorized Amazon personnel.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Amazon performs a vulnerability scan at least once a quarter on Certificate System IP addresses. Amazon will perform a vulnerability scan after any system or network changes that Amazon determines are significant and within one week of receiving a request from the CA/Browser Forum. Amazon will undergo a Penetration Test on Certificate Systems on at least an annual basis and after infrastructure or application upgrades that Amazon determines are significant.

Amazon records will be maintained in a manner reasonably sufficient to demonstrate that each Vulnerability Scan and Penetration Test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

5.5 Records archival

Amazon complies with all record retention policies that apply by law. Amazon includes reasonably sufficient detail in its archived records to show that a certificate or time-stamp token was issued in accordance with this CPS.

5.5.1 Types of records archived

Amazon backs up both application and system data. Amazon may archive the following information:

- audit data, as specified in section 5.4 of this CPS;
- certificate application information;
- documentation supporting a Certificate application; and
- certificate lifecycle information.

5.5.2 Retention period for archive

Amazon retains the records of Amazon digital certificates and the associated documentation for a term of not less than 7 years, or as necessary to comply with applicable laws.

5.5.3 Protection of archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the APPMA or as required by law. Amazon maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If Amazon needs to transfer any media to a different archive site or equipment, Amazon will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4 Archive backup procedures

Amazon maintains backup copies of its archived records at a location distinct from either Certificate Manufacturing Facility.

5.5.5 Requirements for time-stamping of records

Amazon time-stamps archived records with system time (non-cryptographic method) as they are created. Online systems are synchronized with a third party time source using automated means. Air-gapped systems have their time manually set. Manual journal entries have a manually entered date and time.

5.5.6 Archive collection system (internal or external)

Archive information is collected internally by Amazon.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Key changeover procedures enable the smooth transition from expiring CA certificates to new CA certificates. Towards the end of a CA Private Key's lifetime, Amazon ceases using the expiring CA Private Key to sign certificates and uses the expiring Private Key only to sign CRLs and OCSP responder certificates. A new CA signing key pair is commissioned and all subsequently issued certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key certificate is provided to Subscribers and Relying Parties through the delivery methods detailed in 6.1.4 CA Public Key Delivery to Relying Parties. Where Amazon has cross-certified another CA that is in the process of a key rollover, Amazon obtains a new CA Public Key or new CA certificate from the other CA and distributes a new CA cross certificate following the procedures described above.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Amazon maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. Amazon reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

5.7.2 Computing resources, software, and/or data are corrupted

If Amazon discovers that any of its computing resources, software, or data operations have been compromised, Amazon assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If Amazon determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, Amazon suspends such operation until it determines that the risk is mitigated.

5.7.3 Entity private key compromise procedures

In the event a CA Private Key is Compromised, lost, destroyed or suspected to be Compromised, Amazon will, after investigation of the problem, decide if the CA Certificate should be revoked. If so, then all the Subscribers who have currently unrevoked unexpired certificates will be notified at the earliest feasible opportunity. A new CA Key Pair will be generated or an alternative existing CA hierarchy will be used to create new Subscriber Certificates.

If Root CA private keys compromised, Amazon will inform browser vendors of the compromise and best estimate of the date of compromise.

5.7.4 Business continuity capabilities after a disaster

Amazon systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes Amazon PKI operations to become inoperative at one site, Amazon will re-initiate its operations at its alternative site.

5.8 CA or RA termination

Before terminating its CA or TSA activities, Amazon will:

1. Provide notice and information about the termination by sending notice by email to its customers with unrevoked unexpired certificates, Application Software Vendors, and any cross certifying entities and by posting such information on Amazon web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, Amazon will:

1. Transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. Revoke all certificates that are still un revoked or un expired on a date as specified in the notice and publish final CRLs;
3. Destroy all Private Keys; and
4. Make other necessary arrangements that are in accordance with this CPS.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Amazon CA key pairs are generated on hardware that meets the requirements of §6.2.1. They are generated during a ceremony that meets requirements of the Amazon CP.

Subscriber key pairs are generated by the Subscriber.

6.1.2 Private key delivery to subscriber

Amazon does not generate keys for Subscribers and does not distribute Integrated Circuit Cards to subscribers

6.1.3 Public key delivery to certificate issuer

Subscribers generate key pairs and submit the Public Key to Amazon in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the certificate.

6.1.4 CA public key delivery to relying parties

Amazon Public Keys are provided to Relying Parties as trust anchors in commercial browsers and operating system root stores and/or as roots signed by other CAs. All accreditation authorities supporting Amazon certificates and all application software providers are permitted to redistribute Amazon root anchors. Amazon may also distribute Public Keys that are part of an updated signature-Key Pair as a self-signed certificate, as a new CA certificate, or in a key roll over certificate. Relying Parties may obtain Amazon self-signed CA certificates from the Amazon web site.

6.1.5 Key sizes

Amazon CAs use RSA and elliptic curve keys. All RSA keys are 2048-bits or larger and all elliptic curve keys are on one of three NIST curves (P-256, P-384, or P-521).

6.1.6 Public key parameters generation and quality checking

Amazon uses a HSM device that conforms to FIPS 186 2 and provides random number generation and on-board generation of up to 4096 bit RSA Public Keys and a wide range of ECC curves.

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

Amazon includes Key Usage and Extended Key Usage fields in certificates as defined in the certificate profile.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Amazon generates and stores all Private Keys used for certificate signing in cryptographic modules that meet at least one of the following:

- Certified to FIPS 140-1 or 140-2, Level 3 (or higher)
- Certified to ISO/IEC 19790, Level 3 (or higher)
- Certified to EAL4 (or higher) of the CWA 14169 or EN 14169 Protection Profile under the Common Criteria (ISO/IEC 15408) framework

Subscribers must store Private Keys used for Extended Validation Code Signing and Augmented Client certificates in cryptographic modules that meet at least one of the following:

- Certified to FIPS 140-1 or 140-2, Level 2 or higher
- Certified to ISO/IEC 19790, Level 2 or higher
- Certified to EAL4 of the CWA 14169 or EN 14169 Protection Profile under the Common Criteria (ISO/IEC 15408) framework; or
- Certified as a Secure Signature Creation Device (SSCD) by an EU government entity

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

Amazon authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off site and require at least two-person access. Re activation of a backed up CA Private Key (unwrapping) requires the same security and multi person control as when performing other sensitive CA Private Key operations.

6.2.3 Private key escrow

Amazon does not escrow its signature keys and does not provide Subscriber key escrow.

6.2.4 Private key backup

If required for business continuity, Amazon backs up Private Keys under the same multi-person control as the original keys.

6.2.5 Private key archival

Amazon does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module only for backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form.

6.2.7 Private key storage on cryptographic module

Amazon Private Keys are generated and stored inside cryptographic modules which meet the requirements of §6.2.1.

6.2.8 Method of activating private key

Amazon Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure. Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key.

6.2.9 Method of deactivating private key

Amazon Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. Root Private Keys are further deactivated by removing them entirely from the storage partition on the HSM device. Amazon never leaves its HSM devices in an active unlocked or unattended state.

6.2.10 Method of destroying private key

Amazon personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Amazon may destroy a Private Key by deleting it from all known storage partitions. Amazon also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. If the zeroization or re initialization procedure fails, Amazon will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

6.2.11 Cryptographic Module Rating

See §6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Amazon archives copies of Public Keys as specified in §5.5.

6.3.2 Certificate operational periods and key pair usage periods

The lifetime of Amazon's Root CA certificates is as set out in section 1.1. Key pairs in Amazon root certificates have the same term as the certificate validity period. Certificates signed by the CA have a validity period that terminates on or before the end of the validity period of the CA.

6.4 Activation data

6.4.1 Activation data generation and installation

Generation and use of CA activation data used to activate CA Private Keys are made during a key ceremony. Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a holder of a share of the key who is a person in a trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation data protection

CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Amazon PKI systems maintaining CA software and data files are secure from unauthorized access. In addition, access to production servers is limited to those individuals with a valid business reason for such access.

The Amazon PKI production network is separate from other components. This separation prevents network access except through specific application processes. Amazon has access control technologies in place to protect the production network from unauthorized internal and external access and to limit network activities accessing production systems.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Amazon has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. Amazon only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is usually purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by Amazon are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to Amazon operations is scanned for malicious code on first use and periodically thereafter.

6.6.2 Security management controls

Amazon has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, Amazon verifies that the software is the correct version and is supplied by the vendor free of any modifications. Amazon verifies the integrity of software used with its CA processes at least once per week.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

Amazon has implemented reasonable safeguards and controls to prevent unauthorized access to the various systems and devices that comprise the CA infrastructure and to various degrees depending on the sensitivity of the function. Root CA private keys are kept offline and protected by various means.

6.8 Time-stamping

See §5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Amazon uses the ITU X.509, version 3 standard to construct digital certificates for use within the Amazon PKI. Amazon adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995.

7.1 Certificate profile

7.1.1 Version number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate extensions

See Amazon Certificate Profiles appendix.

7.1.3 Algorithm object identifiers

See Amazon Certificate Profiles appendix.

7.1.4 Name forms

Each certificate includes a unique positive serial number that is never reused. Optional subfields in the subject of an SSL Certificate must either contain information verified by Amazon or be left empty. SSL Certificates cannot contain metadata such as '.', '-' and ' ' characters or any other indication that the field is not applicable. Amazon logically restricts OU fields from containing Subscriber information that has not been verified as specified in 3 Identification and Authentication.

The distinguished name for each Certificate type is set forth in Amazon certificate profiles appendix. The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

Certificates that are issued under the Amazon PKI and are compliant with the CA/Browser Forum Baseline Requirements may include the 1.3.187.1 object identifier in their policy list.

Certificates that are issued under the Amazon PKI and are complaint with the CA/Browser Forum Extended Validation Guidelines may include the 1.3.187.1.1 object identifier in the policy list.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

Not applicable.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

7.2.1 Version number(s)

Amazon issues version 2 CRLs.

7.2.2 CRL and CRL entry extensions

Field	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3 OCSP profile

7.3.1 Version number(s)

Amazon OCSP responders conform to version 1 as defined in RFC 6960. Amazon OCSP responders may decline to respond to messages that do not comply with RFC 5019. Specifically, Amazon OCSP responders may not include a nonce in the reply even if a nonce is provided in the request.

7.3.2 OCSP extensions

No stipulations.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest version of the EV Guidelines and the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188").

8.1 Frequency or circumstances of assessment

The WebTrust for CAs audit mandates that the period during which a CA issues Certificates be divided into an unbroken sequence of audit periods. An audit period must not exceed one year in duration.

8.2 Identity/qualifications of assessor

Amazon receives an annual audit by an independent external auditor to assess Amazon compliance with this CPS, any applicable CPs, and the CA WebTrust/ISO 21188 and WebTrust EV Program criteria. The audit covers Amazon operated RA systems, Sub CAs, and OCSP Responders.

WebTrust auditors must meet the requirements of Section 14.1.14 of the EV Guidelines. Specifically:

1. Qualifications and experience: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor, an AICPA Certified Information Technology Professional, a Certified Internal Auditor, or have another recognized information security auditing credential. Auditors must be subject to disciplinary action by its licensing body.
2. Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.
3. Rules and standards: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.
4. Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.
5. Insurance: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

8.3 Assessor's relationship to assessed entity

Amazon's WebTrust auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against Amazon.

8.4 Topics covered by assessment

The audit covers Amazon business practices disclosure, the integrity of Amazon PKI operations, and Amazon compliance with the EV Guidelines. The audit verifies that Amazon is compliant with the CP and this CPS.

8.5 Actions taken as a result of deficiency

If an audit reports a material noncompliance with applicable law, this CPS, the CP, or any other contractual obligations related to Amazon, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify Amazon, and (3) Amazon will develop a plan to cure the noncompliance. Amazon will submit

the plan to the APPMA for approval and to third parties if required by law. The APPMA may require additional action if necessary to rectify any significant issues created by the non- compliance, including requiring revocation of affected certificates.

8.6 Communication of results

The results of each audit are reported to the APPMA, to the public and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. On an annual basis, Amazon submits a report of its audit compliance to various parties, such as Mozilla, Microsoft, CA licensing bodies, etc. Amazon is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

8.7 Self-Audits

On at least a quarterly basis, Amazon performs regular internal audits against a randomly selected sample of at least the greater of 1 certificate or three percent of the certificates issued since the last internal audit. Internal audits on EV Certificates are performed in accordance with section 14.1.2 of the EV Guidelines.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Amazon may charge Subscribers for certificate issuance and renewal.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

Amazon does not charge a certificate revocation fee or a fee for checking the validity status of an issued certificate using a CRL. Amazon may charge a fee for providing certificate status information via OCSP.

9.1.4 Fees for other services

Amazon does not charge Subscribers for revocation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

Amazon maintains insurance or self-insures in accordance with Section 9.2.1 of the CP.

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 information is considered confidential information of Amazon and is protected against disclosure using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by Amazon as private information in accordance with 9.3 Confidentiality of Business Information;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2 Information not within the scope of confidential information

Certificates and revocation data are considered public information. Amazon reserves the right to publish a CRL as may be indicated.

9.3.3 Responsibility to protect confidential information

Amazon employees, agents, and contractors are responsible for protecting confidential information and are bound by Amazon's policies with respect to the treatment of confidential information or are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of personal information

9.4.1 Privacy plan

Amazon follows the privacy policy posted on its website when handling personal information.

9.4.2 Information treated as private

Amazon treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. Amazon protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 Information not deemed private

Certificates and revocation data are not private information.

9.4.4 Responsibility to protect private information

Amazon employees and contractors are subject to policies or contractual obligations requiring such employees and contractors to comply with the Amazon Privacy Policy or contractual obligations at least as protective of private information as the Amazon Privacy Policy.

9.4.5 Notice and consent to use private information

Amazon follows the privacy policy posted on its website when using personal information.

9.4.6 Disclosure pursuant to judicial or administrative process

Amazon will not disclose Subject private information unless required to do so to comply with a legally valid and binding order, such as a subpoena or a court order.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Amazon and/or its business partners own the intellectual property rights in Amazon's services, including the certificates, trademarks used in providing the services, and this CPS. Certificate and revocation information are the property of Amazon. Amazon grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, Amazon does not make any representations or warranties regarding its products or services. Amazon represents and warrants, to the extent specified in this CPS, that:

1. Amazon complies, in all material aspects, with the CP and this CPS,
2. Amazon publishes and updates CRLs and OCSP responses on a regular basis,
3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the Baseline Requirements, and
4. Amazon will maintain a repository of public information on its website.

For EV Certificates, Amazon warrants to Subscribers, Subjects, Application Software Vendors that distribute Amazon root certificates, and Relying Parties that use an Amazon certificate while the certificate is valid that Amazon followed the EV Guidelines in all material respects when verifying information and issuing EV Certificates.

This foregoing warranty is limited solely to Amazon compliance with the EV Guidelines (e.g., Amazon may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the EV Guidelines).

9.6.2 RA representations and warranties

Each RA represents and warrants that:

1. The RA's certificate issuance and management services conform to the Amazon CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All certificates requested by the RA meet the requirements of this CPS.

Amazon's agreement with the RA may contain additional representations and warranties.

9.6.3 Subscriber representations and warranties

Prior to issuance of a certificate, Amazon confirms that either:

1. the applicant has agreed to the Subscriber Agreement or
2. the applicant is an employee or agent of Amazon or an Affiliate of Amazon

At least once every 12 months, the CA confirms that an authorized representative of Amazon has agreed to the Terms of Use.

Subscribers represent and warrant that:

1. each digital signature created using the Private Key corresponding to the Public Key listed in the certificate has been accepted and has not expired or been revoked at the time the digital signature is created;
2. the Subscriber, or someone explicitly authorized by the Subscriber, have been and remain the only person(s) in possession of Subscriber's Private Key and all materials and information protecting Subscriber's Private Key, and no unauthorized person has had or will have access to such materials and information;
3. All material information Subscriber provides to the CA in Subscriber's certificate application or related to the issuance of a certificate is accurate, complete and up to date; and
4. Subscriber's certificates is and will be used in compliance with all applicable laws and in accordance with this CPS, any subscriber agreement between Subscriber and the CA and any applicable standards, including, without limitation, the EV Guidelines, as an end user and not as a CA to issue certificates, certificate revocation lists, or otherwise.

The Subscriber Agreement between the Subscriber and Amazon may include additional representations and warranties.

9.6.4 Relying party representations and warranties

Each Relying Party represents and warrants that, prior to relying on an Amazon certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to Amazon's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the Amazon certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an Amazon certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on an Amazon certificate after considering:

   a. Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction; b. The intended use of the certificate as listed in the certificate or this CPS, c. The data listed in the certificate, d. The economic value of the transaction or communication, e. 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, f. The Relying Party's previous course of dealing with the Subscriber, g. The Relying Party's understanding of trade, including experience with computer-based methods of trade, and h. Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimers of warranties

AMAZON'S SERVICE OFFERINGS IN CONNECTION WITH THIS CPS ARE PROVIDED "AS IS." WE AND OUR AFFILIATES AND LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE OFFERINGS OR ANY THIRD PARTY CONTENT, INCLUDING ANY WARRANTY THAT THE SERVICE OFFERINGS OR THIRD PARTY CONTENT WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR AFFILIATES AND LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF

MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

9.8 Limitations of liability

WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF ANY (I) TERMINATION OR SUSPENSION OF THIS CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS CPS, OR, (III) ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF CA SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS BY YOU IN CONNECTION WITH THIS CPS OR YOUR USE OF OR ACCESS TO AMAZON'S CA SERVICE OFFERINGS; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR CONTENT OR OTHER DATA. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH THIS CPS AND ALL CERTIFICATES ISSUED HEREUNDER, IS LIMITED TO $500; PROVIDED, HOWEVER, THAT FOR ANY EV CERTIFICATE ISSUED UNDER THIS CPS, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IS LIMITED TO $2,000 PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE.

9.9 Indemnities

Indemnification by Amazon

Amazon shall indemnify each Application Software Vendor against any damage or loss suffered by an Application Software Vendor related to or arising out of any third party allegation, claim, lawsuit, or proceeding (a "Claim") to the extent such Claim is based on an EV Certificate issued by Amazon except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

In connection with any Claim described in the foregoing paragraph, the indemnified party will: (a) give Amazon prompt written notice of the Claim (provided that any delay in notification will not relieve Amazon of its indemnity obligations except to the extent that the delay impairs its ability to defend); (b) cooperate reasonably with Amazon (at Amazon's expense) in connection with the defense and settlement of the Claim; and (c) permit Amazon to control the defense and settlement of the Claim, provided that Amazon may not settle the Claim without the indemnified party's prior written consent (which will not be unreasonably

withheld or delayed), and provided further that the indemnified party (at its cost) may participate in the defense and settlement of the Claim with counsel of its own choosing. Amazon's duty to indemnify under this Section 9.9 will be independent from its other obligations under this Agreement.

Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Amazon, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of its Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of a certificate or Private Key.

Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Amazon, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any service terms applicable to the services provided by Amazon or its affiliates and used by the Relying Party, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 Term

This CPS and any amendments to the CPS are effective when published to Amazon online repository and remain in effect until replaced with a newer version.

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

Amazon will communicate the conditions and effect of this CPS's termination via the Amazon Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

9.11 Individual notices and communications with participants

Amazon accepts notices related to this CPS at the locations specified in §2.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from Amazon. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in §2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. Amazon may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS is reviewed at least annually and may be reviewed more frequently. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place that are designed to reasonably ensure that this CPS is not amended and published without the prior authorization of the APPMA .

9.12.2 Notification mechanism and period

Amazon posts CPS revisions to its Repository. Amazon does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited certificates are announced and approved by the accrediting agency prior to becoming effective. The APPMA is responsible for determining what constitutes a material change of the CPS .

9.12.3 Circumstances under which OID must be changed

The APPMA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute resolution provisions

Parties are required to notify Amazon and attempt to resolve disputes directly with Amazon before resorting to any dispute resolution mechanism.

9.14 Governing law

The laws of the state of Washington State govern the interpretation, construction, and enforcement of this CPS and all proceedings related to Amazon products and services, including tort claims, without regard to any conflicts of law principles. The state or federal courts located in King County, Washington have non-exclusive venue and jurisdiction over any proceedings related to the CPS or any Amazon product or service. Amazon may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of our, our affiliates, or any third party's intellectual property or other proprietary rights. The United Nations Convention for the International Sale of Goods does not apply to this CPS.

9.15 Compliance with applicable law

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Amazon contractually obligates each RA to comply with this CPS and applicable industry guidelines. Amazon also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of Amazon. Unless specified otherwise in a contract with a party, Amazon does not provide notice of assignment.

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Amazon may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. Amazon failure to enforce a provision of this CPS does not waive Amazon 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 Amazon.

9.16.5 Force Majeure

Amazon is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond Amazon reasonable control. The operation of the Internet is beyond Amazon's reasonable control.

9.17 Other provisions

No stipulation.

Appendix A: Object Identifiers

Table 1: Signature Algorithms

Name	Object Identifier	Comments
md2WithRSAEncryption	1.2.840.113549.1.1.2	No certificates will be issued with this signature algorithm

Name	Object Identifier	Comments
md4WithRSAEncryption	1.2.840.113549.1.1.3	No certificates will be issued with this signature algorithm
md5WithRSAEncryption	1.2.840.113549.1.1.4	No certificates will be issued with this signature algorithm
sha1WithRSAEncryption	1.2.840.113549.1.1.5	No certificates will be issued with this signature algorithm
sha256WithRSAEncryption	1.2.840.113549.1.1.11	
sha384WithRSAEncryption	1.2.840.113549.1.1.12	
sha512WithRSAEncryption	1.2.840.113549.1.1.13	
rsassaPss	1.2.840.113549.1.1.10	The hash algorithm is specified in the parameters data structure
dsaWithSHA1	1.2.840.10040.4.3	No certificates will be issued with this signature algorithm
dsa_with_SHA256	2.16.840.1.101.3.4.3.2	
ecdsa-with-SHA1	1.2.840.10045.4.1	No certificates will be issued with this signature algorithm
ecdsa-with-SHA256	1.2.840.10045.4.3.2	
ecdsa-with-SHA384	1.2.840.10045.4.3.3	
ecdsa-with-SHA512	1.2.840.10045.4.3.4	

Table 2: Selected Name Attribute Types

Name	Object Identifier	Comments
organizationName	2.5.4.10	Short name: O
countryName	2.5.4.6	Short name: C
organizationalUnitName	2.5.4.11	Short name: OU
commonName	2.5.4.3	Short name: CN
surname	2.5.4.4	Short name: SN
givenName	2.5.4.42	Short name: GN

Appendix B: Certificate Profiles

All certificates from the Amazon PKI must meet the following requirements:

- The Certificate must be a X.509 certificate.
- The version must be v3(2).
- The serial number must be a positive integer
- The validity:notBefore date must be present

- the IssuerUniqueId and subjectUniqueId must not be present
- the signature must be a value from Table 1
- the subjectPublicKeyInfo must be present
- the order of extensions in the certificate may vary
- Names may only have one Attribute per RelativeDistinguishedName
- the Certificate must match one of the below profiles

As described in the Amazon CP, each certificate is categorized as either a CA Certificate or a Subscriber Certificate. Amazon does not issue Subscriber Certificates that simultaneously meet the criteria of multiple of the categories of Subscriber Certificates defined in the CP.

Root CA Certificates

Field	Content
issuer	Must match subject
validity:notAfter	Not more than 25 years after the later of validity:notBefore or the date the certificate was issued
subject	Must contain countryName, organizationName, and commmonName attributes
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey as described in section 4.2.1.2 of RFC5280
extension:basicConstraints	cA is TRUE, pathLenConstraint is not present
extension:keyUsage	digitalSignature, keyCertsign, and cRLSign bits are set, all other bits are not set

The subject Name may have additional attributes such as organizationalUnitName. The subject contents must be validated according to the standard validation rules in section 3.2 of the Certificate Policy. The commonName attribute must contain at least character that a letter, number, ":", "-", ".", or "_" to ensure it is not misinterpreted as a domain name or IP address. For example, the commonName may include a space character to meet this requirement.

Subordinate CA Certificates

Field	Content
validity:notAfter	Not later than the notAfter date of the signing certificate
subject	Must contain countryName, organizationName, and commonName attributes
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey as described in section 4.2.1.2 of RFC5280
extension:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present
extension:certificatePolicies	must contain at least one set of policyInformation containing at least a policyIdentifer

Field	Content
extension:basicConstraints	cA is TRUE
extension:keyUsage	digitalSignature, keyCertsign, and cRLSign bits are set, all other bits are not set
extension:authorityInfoAccess	must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
extension:cRLDistributionPoints	must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

The subject Name may have additional attributes such as organizationalUnitName. The subject contents must be validated according to the standard validation rules in section 3.2 of the Certificate Policy. The commonName attribute must contain at least character that a letter, number, ":", "-", ".", or "_" to ensure it is not misinterpreted as a domain name or IP address. For example, the commonName may include a space character to meet this requirement.

For subordinate CA certificates issued to organizations other than Amazon, the path length constraint in the basicConstraints extensions is set to 0 (zero).

Standard Validation TLS Server Authentication Certificates

Field	Content
serialNumber	If the signatureAlgorithm uses SHA-1, the serial number must contain at least 64 bits of randomly generated entropy
validity:notAfter	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:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 2.23.140.1.2.1
extension:basicConstraints	is either absent or is empty
extension:subjectAltName	must contain at least one name and all names must either be of type dNSName or iPAddress
extension:keyUsage	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extKeyUsage	must include serverAuth, may include clientAuth

Field	Content
extension:authorityInfoAccess	must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
extension:cRLDistributionPoints	must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

The subject and subjectAlternativeName contents must be validated according to the standard validation rules in section 3.2 of the Certificate Policy and comply with CP sections 7.1.4.2 and 7.1.4.3

Extended Validation TLS Server Authentication Certificates

Extended Validation TLS Server Authentication Certificates follow the same profile as Standard Validation TLS Server Authentication Certificates with the following modifications.

Field	Content
validity:notAfter	Not more than 27 months after the later of validity:notBefore or the date the certificate was issued
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 2.23.140.1.1

The subject and subjectAltName contents must be validated according to the extended validation rules of section 3.2 of the Certificate Policy and must comply with CP sections 7.1.4.4 and 7.1.4.5. dNSNames in the subjectAltName may not contain the '*' character.

Standard Validation Code Signing Certificates

Field	Content
serialNumber	If the signatureAlgorithm uses SHA-1, the serial number must contain at least 64 bits of randomly generated entropy
validity:notAfter	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	Must not be empty
extension:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 1.3.187.1
extension:basicConstraints	is either absent or is empty
extension:subjectAltName	a General Name of type permanentIdentifier with an identifierValue present and no assigner value present
extension:keyUsage	digitalSignature bit must be set, other bits should not be set
extension:extKeyUsage	must include codeSigning

Field	Content
extension:authorityInfoAccess	must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
extension:cRLDistributionPoints	must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

The subject and subjectAlternativeName contents must be validated according to the standard validation rules in section 3.2 of the Certificate Policy.

Extended Validation Code Signing Certificates

Extended Validation Code Signing Certificates follow the same profile as Standard Validation Code Signing Certificates with the following modifications.

Field	Content
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 1.3.187.1.1

The subject and subjectAltName contents must be validated according to the extended validation rules of section 3.2 of the Certificate Policy and must comply with CP section 7.1.4.6.

Client Certificates

Field	Content
serialNumber	If the signatureAlgorithm uses SHA-1, the serial number must contain at least 64 bits of randomly generated entropy
validity:notAfter	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	Must not be empty if the subjectAltName is empty
extension:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 1.3.187.1
extension:basicConstraints	is either absent or is empty
extension:subjectAltName	may be present
extension:keyUsage	digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extKeyUsage	must include at least one of clientAuth, emailProtection, Document Signing, or Encrypting Filesystem

Field	Content
extension:authorityInfoAccess	must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
extension:cRLDistributionPoints	must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

For each rfc822Name included in the subjectAltName, the CA ensures that Applicant either has the right to use or controls the email account.

Augmented Client Certificates

Augmented Client Certificates follow the same profile as Client Certificates.

Before issuing an Augmented Client Certificate, the CA confirms that the private key is stored on a device that meets at least one of the following:

- Certified to FIPS 140-1 or 140-2, Level 3 (or higher)
- Certified to ISO/IEC 19790, Level 3 (or higher)
- Certified to EAL4 (or higher) of the CWA 14169 or EN 14169 Protection Profile under the Common Criteria (ISO/IEC 15408) framework
- Certified as a Secure Signature Creation Device (SSCD) by an EU government entity

OCSP Signing Certificates

Field	Content
serialNumber	If the signatureAlgorithm uses SHA-1, the serial number must contain at least 64 bits of randomly generated entropy
validity:notAfter	Not more than 39 months after the later of validity:notBefore or the date the certificate was issued
subject	Must not be empty
extension:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present
extension:certificatePolicies	must contain at least one set of policyInformation containing the policyIdentifier 1.3.187.1
extension:basicConstraints	is either absent or is empty
extension:keyUsage	digitalSignature bit must be set, other bits should not be set
extension:extKeyUsage	must include OCSPSigning
extension:ocsp-nocheck	must be present

Time Stamp Authority Certificates

Field	Content
serialNumber	If the signatureAlgorithm uses SHA-1, the serial number must contain at least 64 bits of randomly generated entropy
validity:notAfter	Not more than 120 months after the later of validity:notBefore or the date the certificate was issued
subject	Must not be empty
extension:basicConstraints	is either absent or is empty
extension:keyUsage	digitalSignature bit must be set, other bits should not be set
extension:extKeyUsage	must include timeStamping
extension:authorityInfoAccess	must contain one AccessDescription with an accessMethod of caIssuers and a Location of type uniformResourceIdentifier and one AccessDescription with an accessMethod of ocsp and a Location of type uniformResourceIdentifier
extension:cRLDistributionPoints	must have at least one DistributionPoint containing a fullName of type uniformResourceIdentifier
extension:authorityKeyIdentifier	keyIdentifier matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber are not present