# Amazon Trust Services - Certificate Policy / Certification Practice Statement (N2) (v1.0)

## 1 INTRODUCTION

### 1.1 Overview

This Certificate Policy ("CP") and Certification Practices Statement ("CPS") is intended to communicate the minimum operating requirements and practices followed by Certification Authority(ies) ("CA(s)") in the Amazon Trust Services PKI ("ATS"). This combined CP and CPS document will be referred to in its entirety as "CP/CPS" unless specific designations to one or the other are necessary for clarity.

This CP/CPS is structured in accordance with IETF RFC 3647 and is designed to conform to the WebTrust Principles and Criteria for Certification Authorities and the WebTrust Principles and Criteria for Certification Authorities – Network Security.

By design, this CP/CPS governs and describes processes for a dedicated set of ATS of CA hierarchies that assert TLS Server Authentication (`id-kp-serverAuth`), TLS Client Authentication (`id-kp-clientAuth`), or both, supporting their use for mutual TLS ("mTLS").

This CP/CPS is only one of several documents that control ATS certification services. Other important documents include both private and public documents, such as ATS's agreements with its customers and ATS's privacy policy. ATS 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 list is not exhaustive.

| **Document** | **Status** | **Location** |
|---|---|---|
| Certificate Policy and Certification Practice Statement | Public | ATS Repository |
| Subscriber Agreement | Public | ATS Repository |
| Relying Party Agreement | Public | ATS Repository |
| Terms of Use | Public | ATS Repository |
| AWS Privacy Policy Public https://aws.amazon.com/privacy/ | Public | |

This CP/CPS, related agreements, and other applicable information referenced within this document is available online at http://www.amazontrust.com/repository.

This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/4.0/.

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

This CP/CPS applies to the following Root Certification Authorities ("Root CAs"):

| **CA Distinguished Name** | **Key pair type and parameters** | **SHA-256 SPKI Fingerprint** | **Validity Period** |
|---|---|---|---|
| C=US, O=Amazon, CN=Amazon N2 RSA 2048 Root M1 | RSA, n has 2048 bits, e=65537 | F0:B7:65:71:8A:EB:03:92:1D:9B:15:83:7F:99:42:0C:35:C7:0B:22:1D:42:75:8E:F6:40:FA:C4:40:67:67:9F | Not Before: 2026-09-02 19:09:23 UTC; Not After: 2046-08-28 19:09:23 UTC |
| C=US, O=Amazon, CN=Amazon N2 RSA 4096 Root M1 | RSA, n has 4096 bits, e=65537 | CA:FD:53:49:90:88:4C:CB:B1:5D:82:55:E4:6E:90:51:A0:28:7A:56:40:ED:37:25:D0:20:2E:08:74:68:B0:69 | Not Before: 2026-09-02 19:09:35 UTC; Not After: 2046-08-28 19:09:35 UTC |
| C=US, O=Amazon, CN=Amazon N2 ECDSA 256 Root M1 | EC, NIST P-256 curve | F8:E8:59:2E:3C:F7:EA:A7:8E:9E:FD:80:6F:2E:AF:EA:77:0B:9F:05:A4:80:33:54:03:25:04:DF:BD:73:93:B8 | Not Before: 2026-09-02 19:09:46 UTC; Not After: 2046-08-28 19:09:46 UTC |
| C=US, O=Amazon, CN=Amazon N2 ECDSA 384 Root M1 | EC, NIST P-384 curve | F7:66:D2:D9:0F:F4:CF:85:CF:FE:91:A4:08:C9:F8:62:64:81:57:A3:CC:D5:76:BE:30:38:2E:EE:A3:DA:6C:48 | Not Before: 2026-09-02 19:09:58 UTC; Not After: 2046-08-28 19:09:58 UTC |

## 1.2 Document name and identification

This document is the ATS CP/CPS. It was approved for publication by the Amazon PKI Policy Management Authority ("APPMA") and is made available at http://www.amazontrust.com/repository. The following revisions were made to the original document:

| Date | Changes | Version |
|---|---|---|
| Oct 28, 2026 | Create published version of the mTLS focused CP/CPS. | 1.0 |

## 1.3 PKI participants

### 1.3.1 Certification authorities

ATS is a CA that issues digital certificates. As a CA, ATS performs functions associated with Public Key operations, including receiving certificate requests, issuing and revoking digital certificates, and maintaining, issuing, and publishing CRLs and OCSP responses. The ATS CA is managed by the APPMA.

### 1.3.2 Registration authorities

ATS may delegate the performance of certain functions to an RA and/or other Delegated Third Parties to request certificates and/or perform identification and authentication for end user certificates. ATS contractually obligates each Delegated Third Party to abide by the policies and industry standards applicable to that Delegated Third Party's role.

### 1.3.3 Subscribers

See definition of "Subscriber" in Section 1.6.1. Prior to verification of identity and issuance of a certificate, a Subscriber is an Applicant.

### 1.3.4 Relying parties

See definition of "Relying Party" in Section 1.6.1. Relying Parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

### 1.3.5 Other participants

If a CA subcontracts CMA, RSP, CSA, or other functions, the CA ensures that compliance with the CP/CPS is required in the agreement with the subcontractor.

## 1.4 Certificate usage

### 1.4.1 Appropriate certificate uses

Certificates issued pursuant to this CP/CPS may be used for authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the certificate, in support of mutual TLS. Each Relying Party must evaluate the application environment and associated risks before relying on a certificate.

### 1.4.2 Prohibited certificate uses

Certificates do not guarantee that the Subject is trustworthy, honest, or reputable. A certificate only establishes that the information in the certificate was verified as

reasonably correct when the certificate was issued. Certificates may not be used (i) for any application requiring fail-safe performance (e.g. nuclear facilities, air traffic control, aircraft navigation, weapons control, or any system whose failure could lead to injury, death, or environmental damage); or (ii) where prohibited by law. Certificates may not be used for "traffic management" or "on-path attack" purposes.

## 1.5 Policy administration

### 1.5.1 Organization administering the document

This CP/CPS and the documents referenced herein are maintained by the APPMA.

### 1.5.2 Contact person

Amazon PKI Policy Management Authority, 410 Terry Ave. North, Seattle, WA 98109-5210. Contact information for Certificate Problem Reports is at http://www.amazontrust.com/repository/.

### 1.5.3 Person determining CP/CPS suitability for the policy

Members of the APPMA determine the suitability and applicability of this CP/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 CP/CPS approval procedures

Members of the APPMA review and approve this CP/CPS and any amendments at least annually.

## 1.6 Definitions and acronyms

### 1.6.1 Definitions

**Affiliate**

A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

**Applicant**

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

**Audit Period**

In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in Section 8.1.

**Authorization Domain Name**

The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

**Base Domain Name**

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

**CA Key Pair**

A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

**Certificate**

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

**Certificate Data**

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

**Certificate Management Process**

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

**Certificate Policy (CP)**

A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

**Certificate Problem Report**

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

**Certificate Profile**

A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7, e.g. a Section in a CA's CPS or a certificate template file used by CA software.

**Certificate Revocation List**

A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

**Certification Authority (CA)**

An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

**Certification Authority Authorization (CAA)**

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

**Certification Practice Statement (CPS)**

One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

**Control**

"Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

**Country**

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

**Cross-Certified Subordinate CA Certificate**

A certificate that is used to establish a trust relationship between two CAs.

**Delegated Third Party**

A natural person or Legal Entity that is not the CA but is authorized by the CA, and whose activities are not within the scope of the appropriate CA audits, to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

**Domain Label**

From RFC 8499 (https://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names."

**Domain Name**

An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

**Domain Name Registrar**

A person or entity that registers Domain Names under the auspices of or by agreement with:

- the Internet Corporation for Assigned Names and Numbers (ICANN),
- a national Domain Name authority/registry, or
- a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

**Fully-Qualified Domain Name (FQDN)**

A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

**Government Entity**

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

**IP Address**

A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

**Issuing CA**

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

**Key Compromise**

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

**Key Generation Script**

A documented plan of procedures for the generation of a CA Key Pair.

**Key Pair**

The Private Key and its associated Public Key.

**Legal Entity**

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

**Multi-Perspective Issuance Corroboration (MPIC)**

A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

**Network Perspective**

Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

**Object Identifier (OID)**

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

**OCSP Responder**

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

**Online Certificate Status Protocol (OCSP)**

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

**Parent Company**

A company that Controls a Subsidiary Company.

**Primary Network Perspective**

The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

**Private Key**

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

**Public Key**

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

**Public Key Infrastructure (PKI)**

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

**Qualified Auditor**

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

**Random Value**

A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

**Registration Authority (RA)**

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

**Relying Party**

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

**Repository**

An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

**Request Token**

A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. The CA SHOULD define within its CPS (or a document clearly referenced by the CPS) the format and method of Request Tokens it accepts.

- The Request Token SHALL incorporate the key used in the certificate request.
- A Request Token MAY include a timestamp to indicate when it was created.
- A Request Token MAY include other information to ensure its uniqueness.
- A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
- A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
- A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.
- The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
- **Note**: Examples of Request Tokens include, but are not limited to:
    i. a hash of the public key; or
    ii. a hash of the Subject Public Key Info [X.509]; or
    iii. a hash of a PKCS#10 CSR.
- A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.
- **Note**: This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR.

```
echo $(date -u +%Y%m%d%H%M) $(sha256sum < r2.csr) | sed "s/[ -]//g"
```

- The script outputs: `201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f`

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

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

**Sovereign State**
A state or country that administers its own government, and is not dependent upon, or subject to, another power.

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

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

**Subscriber**
A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

**Subscriber Agreement**
An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

**Subsidiary Company**
A company that is controlled by a Parent Company.

**Technically Constrained Subordinate CA Certificate**
A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

**Terms of Use**
Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

**Valid Certificate**
A Certificate that passes the validation procedure specified in RFC 5280.

**Validity Period**
From RFC 5280 (https://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive."

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

**Wildcard Certificate**
A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

**Wildcard Domain Name**
A string starting with `*.` (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

### 1.6.2 Acronyms

| Acronym | Meaning |
|---|---|
| CA | Certification Authority |
| CAA | Certification Authority Authorization |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| DNS | Domain Name System |
| FIPS | (US Government) Federal Information Processing Standard |
| FQDN | Fully-Qualified Domain Name |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ISO | International Organization for Standardization |
| mTLS | Mutual Transport Layer Security |
| NIST | (US Government) National Institute of Standards and Technology |

| Acronym | Meaning |
|---|---|
| TLS | Transport Layer Security |

### 1.6.3 References

IETF RFC 3647; RFC 5280; RFC 6960; RFC 8659; NIST SP 800-89; FIPS 140-2 / 140-3; WebTrust Principles and Criteria for Certification Authorities v2.2.3; WebTrust Principles and Criteria for Certification Authorities – Network Security v2.0.5.

### 1.6.4 Conventions

No Stipulation.

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

ATS makes its root certificates, revocation data for issued digital certificates, CPs, CPSs, and standard Subscriber Agreements available in repositories. All updates, amendments, and legal promotions are logged in accordance with the logging procedures referenced in Section 5.4. ATS's legal repository is located at http://www.amazontrust.com/repository. ATS root certificates, CRLs, and OCSP responses are available through online resources 24x7 with systems designed to minimize downtime.

## 2.2 Publication of certification information

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

## 2.3 Time or frequency of publication

New or updated versions of this CP/CPS are typically published to the ATS repository within seven days of approval by the APPMA. This CP/CPS is reviewed at least annually and incrementally versioned even if no changes are made. New or updated Subscriber Agreements or Relying Party representations are typically published within seven days after approval. CA certificates are published typically within seven days of issuance. CRLs are published in accordance with Section 4.9.7.

## 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

See Section 7.1 for the types of names which may appear in this certificate hierarchy.

### 3.1.2 Need for names to be meaningful

No stipulation.

### 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 interpretation as URIs and HTTP references. Certificates do not assert any specific relationship between the subscriber and registrant(s) of DNS name(s). A Certificate may contain a Wildcard Domain Name; the leading "*." represents one or more left-most labels of the domain and is interpreted accordingly.

### 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 the intellectual property rights of another entity. ATS does not verify an Applicant's right to use a trademark and may reject any application or require revocation of any certificate that is part of a trademark dispute.

## 3.2 Initial identity validation

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

### 3.2.1 Method to prove possession of private key

No stipulation.

### 3.2.2 Authentication of organization identity

ATS confirms that the Applicant controls each requested domain name prior to issuance. ATS validates domain control using one or more of the following methods:

1. Confirming control via a DNS record — ATS verifies that the Applicant has placed a CA-provided random value or request token in a DNS record under the domain name being validated (TLS Baseline Requirements Section 3.2.2.4.7).
2. Confirming control via a change to a website — ATS verifies that the Applicant has placed a CA-provided random value at a predetermined path on a website associated with the domain name being validated (TLS Baseline Requirements Section 3.2.2.4.18).

For a Wildcard Domain Name, ATS removes the "*." prefix to yield the corresponding Fully-Qualified Domain Name (the Authorization Domain Name) and validates control of that domain using the DNS-record method described above. ATS corroborates each domain-control validation from multiple network perspectives prior to issuance. ATS maintains records of the domain-control validation performed for each certificate. Validation for Wildcard Domain Names is only performed using the DNS Change method.

### 3.2.3 Authentication of individual identity

Not applicable.

### 3.2.4 Non-verified subscriber information

Not applicable.

### 3.2.5 Validation of authority

Not applicable.

### 3.2.6 Criteria for interoperation

ATS discloses all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject by placing copies in the Repository.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

See section 4.7.

### 3.3.2 Identification and authentication for re-key after revocation

See section 4.7.

## 3.4 Identification and authentication for revocation request

Identification and authentication for revocation requests is performed as described in Section 4.9

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application

Any Applicant or authorized Certificate Requester that is a customer of ATS Web Services (or an authorized reseller) may submit certificate requests. Applicants are responsible for the accuracy of submitted data.

### 4.1.2 Enrollment process and responsibilities

The enrollment process includes submitting a certificate application, generating a key pair, delivering the public key to ATS, agreeing to the applicable Subscriber Agreement, and paying any applicable fees. Prior to issuance, ATS obtains a certificate request in a form prescribed by ATS that certifies the information contained therein is correct.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

ATS verifies the application information specified in Section 3.2.2 and checks the request against an internal database of previously revoked certificates and rejected requests. ATS checks for CAA records for each requested DNS name and processes them in accordance with RFC 8659, honoring the record's TTL. ATS recognizes amazon.com, amazontrust.com, awstrust.com, amazonaws.com, amazontrustservices.eu, amazonaws.eu, and amznts.eu in CAA records (and FQDNs subordinate to these names).

### 4.2.2 Approval or rejection of certificate applications

Approval requires successful completion of validation per Section 3.2.2 as well as compliance with all CA policies.

### 4.2.3 Time to process certificate applications

No stipulation.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

Certificate issuance is authorized by ATS following successful completion of validation under Section 3.2 and application processing under Section 4.2.

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

ATS will deliver certificates within a reasonable time after issuance.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

A Subscriber is deemed to have accepted a certificate when it is used or when no objection is raised within a reasonable time after delivery.

### 4.4.2 Publication of the certificate by the CA

See Section 2.2 for Root and Subordinate CA certificate publication information.

All Subscriber Certificates are made available to Subscribers via an API.

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

See Section 4.4.2.

## 4.5 Key pair and certificate usage

### 4.5.1 Subscriber private key and certificate usage

Subscribers and Relying Parties use key pairs and certificates in accordance with Sections 1.4 and 9.6 and the applicable Subscriber Agreement.

### 4.5.2 Relying party public key and certificate usage

Relying Parties should fully evaluate the context in which they are relying on certificates and the information contained in them, and decide to what extent the risk of reliance is acceptable. If the risk of relying on a certificate is determined to be unacceptable, then Relying Parties should not use the certificate or should obtain additional assurances before using the certificate.

ATS does not warrant that any software used by Relying Parties to evaluate or otherwise handle certificates does so properly.

## 4.6 Certificate renewal

ATS processes renewal, re-key, and modification requests following the same identification and authentication procedures as initial issuance (Section 3.2).

### 4.6.1 Circumstance for certificate renewal

Not applicable.

### 4.6.2 Who may request renewal

Not applicable.

### 4.6.3 Processing certificate renewal requests

Not applicable.

### 4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

### 4.6.6 Publication of the renewal certificate by the CA

Not applicable.

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

Not applicable.

## 4.7 Certificate re-key

ATS processes renewal, re-key, and modification requests following the same identification and authentication procedures as initial issuance (Section 3.2).

### 4.7.1 Circumstance for certificate re-key

Not applicable.

### 4.7.2 Who may request certification of a new public key

Not applicable.

### 4.7.3 Processing certificate re-keying requests

Not applicable.

### 4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

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

Not applicable.

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

Not applicable.

## 4.8 Certificate modification

ATS processes renewal, re-key, and modification requests following the same identification and authentication procedures as initial issuance (Section 3.2).

### 4.8.1 Circumstance for certificate modification

Not applicable.

### 4.8.2 Who may request certificate modification

Not applicable.

### 4.8.3 Processing certificate modification requests

Not applicable.

### 4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

### 4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

### 4.8.6 Publication of the modified certificate by the CA

Not applicable.

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

Not applicable.

## 4.9 Certificate revocation and suspension

ATS supports Certificate Revocation. Certificate suspension is not used.

### 4.9.1 Circumstances for revocation

Prior to revoking a certificate, ATS verifies the identity and authority of the entity requesting revocation. ATS may revoke any certificate in its sole discretion, including:

- Key Compromise;
- Subscriber Revocation Requests;
- Domain Owner Revocation Requests;
- Certificate Problem Reports;
- Issuing CA Revocation Operation;
- Subordinate Operator Request; and
- Subordinate Problem Report.

ATS revokes certificates in a reasonable timeframe after receiving an approved revocation request, usually within 24 hours.

### 4.9.2 Who can request revocation

A revocation request may be submitted by an authenticated Subscriber; by a party able to demonstrate current control over a domain name in the Certificate; by the operator of a Subordinate CA (for the Subordinate CA Certificates it operates); or by any party reporting a suspected problem through ATS's Certificate Problem Report mechanism. ATS may also initiate revocation of any Certificate it has issued. A report of Key Compromise may be submitted by the Subscriber, a Relying Party, or any other third party. ATS authenticates revocation requests as described in Section 3.4.

### 4.9.3 Procedure for revocation request

ATS logs each revocation request or problem report it receives, together with the identity of the requester and the reason given. Requests authenticated as originating from the Subscriber, and requests accompanied by a demonstration of domain control or by the compromised Private Key, are acted upon directly; other reports are investigated before ATS determines whether revocation is warranted. ATS maintains a continuously available capability to receive and respond to high-priority revocation requests.

### 4.9.4 Revocation request grace period

A Subscriber is expected to request revocation promptly after becoming aware of a reason to do so, and without undue delay following detection of a suspected Private Key compromise.

### 4.9.5 Time within which CA must process the revocation request

ATS begins processing a revocation request or problem report usually within 24 hoursreceipt and completes revocation within a timeframe appropriate to the nature of the request, acting on confirmed Private Key compromise without delay. For reports that require investigation, ATS acknowledges the report, keeps the reporter informed of progress, and completes its investigation within the timeframes it maintains for that purpose.

### 4.9.6 Revocation checking requirement for relying parties

Prior to relying on a certificate, a Relying Party must confirm the validity of each certificate in the path in accordance with IETF PKIX standards, including revocation status through CRLs or OCSP responders identified in each certificate.

### 4.9.7 CRL issuance frequency (if applicable)

ATS makes CRLs available via a publicly-accessible HTTP URL. Within 24 hours of issuing its first Certificate, ATS generates and publishes either a full and complete CRL or partitioned CRLs. For Subscriber Certificates, ATS updates and publishes a new CRL at least every seven (7) days (or every four (4) days where certificates do not include an AIA OCSP pointer), and within 24 hours after recording a Certificate as revoked. For CA Certificates, ATS updates and publishes a new CRL at least every twelve (12) months, and within 24 hours after recording a revocation.

### 4.9.8 Maximum latency for CRLs (if applicable)

CRLs are posted to the online repository within a commercially reasonable time after generation and prior to the nextUpdate field of 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 under normal operating conditions.

### 4.9.9 On-line revocation/status checking availability

ATS makes certificate status information available via OCSP for all certificates it issues. OCSP responses conform to RFC 6960 and/or RFC 5019 and are signed by the issuing CA or by an OCSP Responder whose certificate is signed by the issuing CA (with id-pkix-ocsp-nocheck).

### 4.9.10 On-line revocation checking requirements

OCSP responders support the HTTP GET method (RFC 6960 / RFC 5019) and may process the Nonce extension (RFC 8954). For Subscriber Certificates, OCSP responses have a validity interval of at least eight hours and no more than ten days, with update timing as specified for intervals below and at or above sixteen hours. For Subordinate CA Certificates, status is updated at least every twelve months and within 24 hours after revocation. If the responder receives a request for a serial number that is "unused", it will not respond with a "good" status.

### 4.9.11 Other forms of revocation advertisements available

No stipulation.

### 4.9.12 Special requirements re key compromise

See Section `4.9.1` for circumstances related to revocation.

Contact information for reporting private key compromise can be found at:

http://www.amazontrust.com/repository

Proof of key compromise should be submitted by providing the private key itself through the reporting mechanism described on the ATS repository page.

### 4.9.13 Circumstances for suspension

ATS does not suspend certificates.

### 4.9.14 Who can request suspension

Not applicable.

### 4.9.15 Procedure for suspension request

Not applicable.

### 4.9.16 Limits on suspension period

Not applicable.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

Revocation entries on a CRL are not removed until they have appeared in at least one CRL issued after the NotAfter date of the revoked Certificate.

### 4.10.2 Service availability

All certificate status services are made available at all times (24x7) if possible.

### 4.10.3 Optional features

No stipulation.

## 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

ATS 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, Germany, and Ireland. Private keys for all CAs following this CP/CPS are exclusively located in the United States unless otherwise stated in the Repository. Physical barriers, multi-factor access control, two-person access for all access to CA systems, environmental controls (HVAC, water, and fire protection), secure media storage, and secure waste disposal (physical destruction or secure overwriting of media; locked shred bins for documents) are in place. Off-site backups of CA private keys and activation data are stored in devices validated as meeting FIPS 140 Level 3, accessible only by trusted personnel.

### 5.1.2 Physical access

Physical access to ATS Secure PKI Facilities is restricted to authorized Amazon employees, vendors, and contractors, for whom access is required in order to execute their jobs. Access restrictions are strongly enforced via multi-factor authentication mechanisms.

### 5.1.3 Power and air conditioning

Redundant power sources are readily available at each Secure PKI Facility, and are designed to meet ATS's operating requirements.

Air conditioning systems at each Secure PKI Facility are designed to meet ATS's operating requirements.

### 5.1.4 Water exposures

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

### 5.1.5 Fire prevention and protection

ATS's facilities are designed to provide fire suppression for CA systems.

### 5.1.6 Media storage

ATS'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

ATS 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

ATS implements trusted role requirements through a Trusted Role Actions model rather than assigning personnel to standing named roles. Any access to CA systems or hardware that may affect the issuance, use, or revocation of certificates is treated as a trusted role action. Personnel are granted such access only when assigned a specific action to perform, and only for as long as needed to perform it. Trusted role actions are assigned through controlled mechanisms that provide documented instructions, peer review, monitoring, and multi-person control where applicable, so that personnel act only within the scope of the actions assigned to them and no single individual can independently perform all critical CA operations.

### 5.2.2 Number of persons required per task

Trusted Role Actions that are security-sensitive are performed under multi-person control. No single individual can independently perform all critical CA operations, and two-person verification is required where applicable — including for CA key generation, CA signing key activation, and CA private key backup.

### 5.2.3 Identification and authentication for each role

Personnel are identified and authenticated at the point a Trusted Role Action is assigned and access to the applicable CA software or hardware is granted. Access is granted only for the assigned action and is not persistent.

### 5.2.4 Roles requiring separation of duties

Trusted Role Actions are assigned under the principles of least privilege and separation of duties. Personnel act only within the scope of the Trusted Role Action(s) assigned to them, and the assignment mechanisms are structured so that no single individual can both authorize and solely execute a critical CA operation.

## 5.3 Personnel controls

### 5.3.1 Qualifications, experience, and clearance requirements

ATS ensures that personnel assigned Trusted Role Actions have the experience, qualifications, and trustworthiness required to perform them. Personnel act only within the scope of the Trusted Role Action(s) assigned to them.

### 5.3.2 Background check procedures

All personnel must have completed and passed a background check prior to being hired.

### 5.3.3 Training requirements

ATS provides personnel with task-specific training at the point they are assigned a trusted role action, rather than through a separate general training program. The controlled mechanisms used to assign a trusted role action also deliver the instructions and the applicable control requirements for that action, so that personnel are trained on the specific action they are about to perform. Personnel receive the training appropriate to their assigned actions before performing them.

### 5.3.4 Retraining frequency and requirements

Because training is tied to each assigned action, personnel receive current instruction at least on or before the first time they are assigned a trusted role action. ATS updates this instruction as its practices, systems, or applicable requirements change, so that personnel apply the current procedures and controls when they next perform an action.

### 5.3.5 Job rotation frequency and sequence

No stipulation.

### 5.3.6 Sanctions for unauthorized actions

ATS employees and agents failing to comply with this CP/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 performing a trusted role action are provided with the documentation necessary to perform their duties, including a copy of the CP/CPS, and other technical and operational documentation needed to maintain the integrity of ATS CA operations.

## 5.4 Audit logging procedures

### 5.4.1 Types of events recorded

Audit logs are generated for all events related to CA security (physical and logical) and certificate issuance. Logs are automatically generated whenever possible. When it is necessary to manually log information, logs are kept on paper with written confirmation from a witness and securely stored. All audit logs, electronic or otherwise, shall be retained and made available to compliance auditors upon request.

At a minimum, each audit record includes:

- Date and time of entry;
- Identity of the person (or machine) making the entry; and
- Description of the entry.

### 5.4.2 Frequency of processing log

No stipulation.

### 5.4.3 Retention period for audit log

Audit logs are retained for at least two years and will be made available to the ATS 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

ATS 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, ATS Administrators will consider suspending its operation until the problem is remedied. Manually generated audit data is recorded by authorized ATS personnel.

### 5.4.7 Notification to event-causing subject

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

### 5.4.8 Vulnerability assessments

ATS performs a vulnerability scan at least once a quarter on CA systems, after any significant system or network change, and within one week of receiving a request from the APPMA. ATS undergoes a Penetration Test on CA systems at least annually and after significant infrastructure or application upgrades. ATS maintains records sufficient to demonstrate each scan and test was performed by a qualified, independent person or entity.

## 5.5 Records archival

### 5.5.1 Types of records archived

ATS archives all audit logs, the contents of which are described in Section 5.4.1. ATS also archives other documents and information critical to understanding the historical security and performance of the CA's duties.

### 5.5.2 Retention period for archive

ATS retains the records of ATS digital certificates and the associated documentation for a term of not less than 5 years, or as necessary to comply with applicable laws.

### 5.5.3 Protection of archive

Archives are protected from unauthorized modification or destruction by strong security and environmental controls.

### 5.5.4 Archive backup procedures

Archives are backed up regularly.

### 5.5.5 Requirements for time-stamping of records

ATS time-stamps archived records with system time (a 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)

No Stipulation.

### 5.5.7 Procedures to obtain and verify archive information

No Stipulation.

## 5.6 Key changeover

See Section 6.1.

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

ATS maintains an Incident Response Plan and a Disaster Recovery Plan, and documents business continuity and disaster recovery procedures designed to notify and reasonably protect relevant stakeholders, Subscribers, and Relying Parties. The business continuity plan is tested, reviewed, and updated at least annually and includes activation conditions, emergency/fallback/resumption procedures, a maintenance schedule, recovery time objectives, off-site storage of critical cryptographic materials, and related elements. ATS maintains a mass revocation plan tested annually. If computing resources, software, or data are compromised, ATS assesses the risk and suspends affected operations until mitigated.

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

If ATS discovers that any of its computing resources, software, or data operations have been compromised, ATS assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If ATS determines that

a continued operation could pose a significant risk to Relying Parties or Subscribers, ATS 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, ATS 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.

### 5.7.4 Business continuity capabilities after a disaster

ATS 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 ATS operations to become inoperative at one site, ATS will re-initiate its operations at its alternative site.

## 5.8 CA or RA termination

Before terminating its CA activities, ATS will provide notice to its customers with unrevoked unexpired certificates and any cross-certifying entities, post such information on its web site, and transfer all responsibilities to a qualified successor entity. If none exists, ATS will transfer transferable functions to a reliable third party, preserve relevant records, revoke all unrevoked/unexpired certificates and publish final CRLs, and destroy all Private Keys.

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

ATS CA Private Keys are generated by HSMs meeting the specifications described in Section 6.2.1. This occurs during a ceremony meeting the requirements of this CP/CPS.

See the ATS Subscriber Agreement for information regarding Subscriber key pair generation. Once submitted as part of a certificate request, Subscriber Public Keys are rejected if they do not meet requirements of Section 6.1.5 and Section 6.1.6, can be easily compromised by certain attacks (including Debian weak keys, ROCA, and Close Primes vulnerabilities), or appear in our database of known-weak and known-compromised keys.

### 6.1.2 Private key delivery to subscriber

ATS does not generate keys for Subscribers.

### 6.1.3 Public key delivery to certificate issuer

Subscribers generate key pairs and submit the Public Key to ATS 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

ATS Public Keys are available on the repository: http://www.amazontrust.com/repository

### 6.1.5 Key sizes

For RSA key pairs, ATS ensures the modulus is at least 2048 bits and evenly divisible by 8. For ECDSA key pairs, ATS ensures the key represents a valid point on the NIST P-256, P-384, or P-521 curve.

### 6.1.6 Public key parameters generation and quality checking

RSA: ATS confirms the public exponent is an odd number ≥ 3 (between 2^16+1 and 2^256−1) and that the modulus is odd, not a prime power, and has no factors smaller than 752 (NIST SP 800-89). [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: ATS confirms key validity using the ECC Full or Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

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

See Section 7.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic module standards and controls

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

- Certified to FIPS 140-3, 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

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

Private keys are protected by multi-person control; backups are stored off-site and require at least two-person access.

### 6.2.3 Private key escrow

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

### 6.2.4 Private key backup

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

### 6.2.5 Private key archival

ATS 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

ATS CA Private Keys are stored on HSMs meeting the specifications described in Section 6.2.1.

### 6.2.8 Method of activating private key

ATS CA Private Keys are always stored on HSMs and activated using the mechanisms provided by the HSM manufacturer.

### 6.2.9 Method of deactivating private key

ATS CA Private Keys are always stored on HSMs and deactivated using the mechanisms provided by the HSM manufacturer.

### 6.2.10 Method of destroying private key

ATS personnel, performing a trusted role action, destroy CA, RA, and status server Private Keys when no longer needed. ATS may destroy a Private Key by deleting it from all known storage partitions. ATS 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, ATS 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 Section 6.2.1 of this CP/CPS.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

ATS archives copies of Public Keys as specified in Section 5.5 of this CP/CPS.

### 6.3.2 Certificate operational periods and key pair usage periods

The lifetime of ATS's Root CA certificates is as set out in Section 1.1; key pairs in ATS root certificates have the same term as the certificate validity period. The validity period of Subscriber Certificates is 398 days or less.

## 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 performing a trusted role action. 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

ATS systems maintaining CA software and data files are secured from unauthorized access. ATS enforces multi-factor authentication for all accounts capable of directly causing certificate issuance and maintains a security framework governing the technical aspects of its computer security.

### 6.5.2 Computer security rating

No Stipulation.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

ATS controls and monitors the acquisition and development of its CA systems. Changes to CA systems are reviewed and approved by someone other than the person requesting the change, and CA hardware and software are dedicated to the operation of the CA. Software developed for the CA is produced in a controlled environment following a defined development process, and software and equipment are obtained and delivered in a manner designed to prevent tampering.

### 6.6.2 Security management controls

ATS controls and monitors the security-related configuration of its CA systems. The integrity of CA systems and their configuration is maintained, changes are tracked, and systems are checked for unauthorized modification and for malicious code.

### 6.6.3 Life cycle security controls

See Section 6.5.1 of this CP/CPS.

## 6.7 Network security controls

ATS has implemented reasonable safeguards and controls to prevent unauthorized access to the systems and devices that comprise the CA infrastructure. Root CA private keys are kept offline. All CA and RA systems are protected in accordance with the applicable WebTrust Principles and Criteria for Certification Authorities – Network Security. Vulnerability remediation timelines are governed by severity: Emergent — immediate investigation until mitigated; Critical and High/Important — 30 days; Medium/Moderate — 60 days; Low — 120 days. Exceptions are assessed for risk and documented.

## 6.8 Time-stamping

See Section 5.5.5 of this CP/CPS.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profile

All ATS Certificates are issued in accordance with one of the following Certificate Profiles

### Root Certificate Profile

| Field / Extension | Value |
|---|---|
| version | v3 |

| | |
|---|---|
| serialNumber | Non-sequential; at least 64 bits of CSPRNG output; up to 20 octets |
| issuer / subject | Identical (self-signed). C=US (or DE), O=Amazon, CN of the form “Amazon N2 <RSA 2048\|RSA 4096\|ECDSA 256\|ECDSA 384> Root M1” |
| validity | 20 years (notBefore to notAfter) |
| subjectPublicKeyInfo | RSA ≥ 2048 bits, or NIST P-256 / P-384 |
| signatureAlgorithm | SHA-256 or SHA-384 with RSA or ECDSA (no MD5, SHA-1, or RSA-with-SHA-1) |
| keyUsage | critical; digitalSignature, keyCertSign, cRLSign |
| basicConstraints | critical; cA=TRUE; no pathLenConstraint |
| subjectKeyIdentifier | present; non-critical; SHA-1 of the subjectPublicKey |
| authorityKeyIdentifier | when present, non-critical and equal to the subjectKeyIdentifier |
| extendedKeyUsage | not present |
| certificatePolicies | not present |

## Subordinate CA Certificate Profile

| **Field / Extension** | **Value** |
|---|---|
| version | v3 |
| serialNumber | Non-sequential; at least 64 bits of CSPRNG output; up to 20 octets |
| issuer | Subject DN of the issuing Root CA, byte-for-byte |
| subject | C=US (or DE), O=Amazon, CN of the form “Amazon N2 <key type> M00n” |
| validity | 3 years (1095 days) |
| subjectPublicKeyInfo | RSA ≥ 2048 bits, or NIST P-256 / P-384 |
| signatureAlgorithm | SHA-256 or SHA-384 with RSA or ECDSA |
| keyUsage | critical; digitalSignature, keyCertSign, cRLSign |
| basicConstraints | critical; cA=TRUE; pathLenConstraint=0 |
| extendedKeyUsage | non-critical; id-kp-serverAuth and, optionally, id-kp-clientAuth; anyExtendedKeyUsage and all other key purposes are excluded |
| certificatePolicies | non-critical; the ATS mTLS CP/CPS policy identifier 1.3.187.121.1.20 |
| subjectKeyIdentifier | present; non-critical; SHA-1 of the subjectPublicKey |
| authorityKeyIdentifier | present; non-critical; keyIdentifier of the issuing Root CA |
| cRLDistributionPoints | present; non-critical; HTTP URI of the issuing CA’s CRL |
| authorityInformationAccess | present; non-critical; OCSP URI and caIssuers URI of the issuing CA |
| nameConstraints | not present |

### End-Entity (Subscriber) Certificate Profile

| Field / Extension | Value |
|---|---|
| version | v3 |
| serialNumber | Non-sequential; at least 64 bits of CSPRNG output; up to 20 octets |
| issuer | Subject DN of the issuing Subordinate CA, byte-for-byte |
| subject | May be empty (with a critical SAN) or contain only commonName and/or countryName; organization, locality, state, street, and postalCode are not present |
| validity | 395 days |
| subjectPublicKeyInfo | RSA ≥ 2048 bits, or NIST P-256 / P-384 |
| signatureAlgorithm | SHA-256 or SHA-384 with RSA or ECDSA |
| keyUsage | critical; digitalSignature (RSA may add keyEncipherment for legacy TLS 1.2 RSA key exchange); keyCertSign and cRLSign are not set |
| extendedKeyUsage | non-critical; at least one of id-kp-serverAuth and id-kp-clientAuth, and no other key purpose |
| certificatePolicies | non-critical; optionally, the ATS mTLS CP/CPS policy identifier 1.3.187.121.1.20 |
| subjectAltName | one or more dNSName values; may include a Wildcard Domain Name as the left-most label (e.g. *.example.com); no IP-address, rfc822Name, otherName, or directoryName values; critical when the subject DN is empty |
| basicConstraints | when present, cA=FALSE; no pathLenConstraint |
| authorityKeyIdentifier | present; non-critical; keyIdentifier of the issuing CA |
| authorityInformationAccess | present; non-critical; OCSP URI and caIssuers URI |
| cRLDistributionPoints | present; non-critical; HTTP URI of the issuing CA's CRL (optional for short-lived certificates) |
| subjectKeyIdentifier | not present |

### 7.1.1 Version number(s)

All certificates are X.509 version 3 certificates.

### 7.1.2 Certificate extensions

See Section 7.1.

### 7.1.3 Algorithm object identifiers

ATS issues certificates with algorithms described by the following OIDs:

| Name | Object Identifier |
|---|---|
| sha256WithRSAEncryption | 1.2.840.113549.1.1.11 |
| sha384WithRSAEncryption | 1.2.840.113549.1.1.12 |
| sha512WithRSAEncryption | 1.2.840.113549.1.1.13 |
| 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 |

ATS does not issue any Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm.

### 7.1.4 Name forms

ATS issues certificates with name forms that comply with RFC5280.

### 7.1.5 Name constraints

No stipulation.

### 7.1.6 Certificate policy object identifier

See Section 7.1

### 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

This profile applies to CRLs issued by ATS subordinate (issuing) CAs in the mTLS hierarchy for the Subscriber certificates they issue. Each CRL is signed by the CA that issued the certificates it covers; ATS does not issue indirect CRLs.

### CRL profile field

| Field / Extension | Value |
|---|---|
| version | v2 (integer value 1) |

| | |
|---|---|
| signatureAlgorithm | SHA-256 or SHA-384 with RSA or ECDSA, matching the issuing CA's key; identical in the tbsCertList and the CertificateList |
| issuer | The Subject DN of the issuing CA, byte-for-byte; C=US (or DE), O=Amazon, CN of the issuing CA |
| thisUpdate | Issue date of the CRL; may be backdated by no more than four hours |
| nextUpdate | Subordinate CA CRLs covering Subscriber certificates: 7 days after thisUpdate if every certificate in scope carries an OCSP AIA (id-ad-ocsp), otherwise 4 days. Root CA CRL values are pending verification against the root-tier profile. |
| revokedCertificates | Present when at least one revoked certificate remains on a regularly scheduled CRL after its validity period; each entry carries serialNumber, revocationDate, and optional reasonCode |
| crlExtensions | Present (see Section 7.2.2) |
| signature | Computed by the issuing CA over the DER-encoded tbsCertList |

### CRL and CRL entry extensions

| Field / Extension | Value |
|---|---|
| authorityKeyIdentifier | non-critical; keyIdentifier of the issuing CA, equal to its subjectKeyIdentifier |
| cRLNumber | non-critical; non-negative integer, strictly increasing across successive CRLs from the same issuer |
| issuingDistributionPoint | used only for partitioned CRLs; critical; onlyContainsUserCerts or onlyContainsCACerts (not both); indirectCRL FALSE; not used for full and complete CRLs |
| reasonCode (CRL entry) | non-critical; permitted values listed in Section 7.2.3; omitted when the reason is unspecified (0) |

### 7.2.1 Version number(s)

ATS issues version 2 CRLs.

### 7.2.2 CRL and CRL entry extensions

No stipulation.

## 7.3 OCSP profile

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

### 7.3.1 Version number(s)

No stipulation.

### 7.3.2 OCSP extensions

No stipulation.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CP/CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the WebTrust for Certification Authorities principles and criteria.

## 8.1 Frequency or circumstances of assessment

WebTrust compliance audits are performed at least annually in a contiguous, unbroken sequence. Self-audits are performed as described in Section 8.7 of this document.

## 8.2 Identity/qualifications of assessor

ATS's WebTrust auditors must meet the requirements listed here for reference:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an eligible audit scheme (see Section 8.4);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

## 8.3 Assessor's relationship to assessed entity

ATS'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 ATS.

## 8.4 Topics covered by assessment

The WebTrust audit covers ATS business practices disclosure, the integrity of ATS operations, and verifies ATS is compliant with this CP/CPS.

## 8.5 Actions taken as a result of deficiency

Noncompliance with relevant requirements will be documented by auditors (internal or external), the AAPMA will be informed, and the AAPPMA will ensure that steps are taken to address the issues as quickly as reasonably possible.

## 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, ATS submits a report of its audit compliance to applicable parties. ATS is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

## 8.7 Self-Audits

ATS monitors adherence to this CP/CPS and performs self-audits at least quarterly against a randomly selected sample of the greater of one certificate or three percent of the Certificates issued since the previous sample. ATS controls the service quality of Certificates verified by Delegated Third Parties through ongoing quarterly audits and reviews each Delegated Third Party's compliance with this CP/CPS at least annually.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

### 9.1.1 Certificate issuance or renewal fees

ATS 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

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

### 9.1.4 Fees for other services

No Stipulation.

### 9.1.5 Refund policy

ATS refunds customers for erroneous charges.

## 9.2 Financial responsibility

### 9.2.1 Insurance coverage

No Stipulation.

### 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

No Stipulation.

### 9.3.2 Information not within the scope of confidential information

No Stipulation.

### 9.3.3 Responsibility to protect confidential information

ATS employees, agents, and contractors are responsible for protecting confidential information and are bound by ATS'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

ATS follows the Amazon Web Services Privacy Notice posted on the AWS website when handling personal information.

### 9.4.2 Information treated as private

ATS treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. ATS 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

ATS 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

ATS follows the Amazon Web Services Privacy Notice posted on the AWS website when handling personal information.

### 9.4.6 Disclosure pursuant to judicial or administrative process

ATS will not disclose Subject private information except as specified on the Amazon Web Services Privacy Notice posted on the AWS website.

### 9.4.7 Other information disclosure circumstances

ATS will not disclose Subject private information except as specified on the Amazon Web Services Privacy Notice posted on the AWS website.

## 9.5 Intellectual property rights

ATS and/or its affiliates and business partners own the intellectual property rights in ATS's services, including certificates, trademarks, and this CP/CPS. ATS grants permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis provided they are reproduced in full. Private 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 CP/CPS or in a separate agreement with a Subscriber, ATS does not make any representations or warranties regarding its products or services. ATS represents and warrants, to the extent specified in this CP/CPS, that:

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

### 9.6.2 RA representations and warranties

ATS does not use RA services from third parties.

### 9.6.3 Subscriber representations and warranties

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

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

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 CP/CPS, any subscriber agreement between Subscriber and the CA and any applicable standards, including, without limitation, as an end user and not as a CA to issue certificates, certificate revocation lists, or otherwise.

The Subscriber Agreement between the Subscriber and ATS 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 ATS 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 ATS's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CP/CPS,
4. Verified both the ATS certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an ATS 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 ATS 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 CP/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 CP/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 CP/CPS OR REVOCATION OF A CERTIFICATE, (II) OUR DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS CP/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 CP/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.

## 9.9 Indemnities

In connection with any Claim described in the foregoing paragraph, the indemnified party will: (a) give ATS prompt written notice of the Claim (provided that any delay in notification will not relieve ATS of its indemnity obligations except to the extent that the delay impairs its ability to defend); (b) cooperate reasonably with ATS (at ATS's expense) in connection with the defense and settlement of the Claim; and (c) permit ATS to control the defense and settlement of the Claim, provided that ATS 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. ATS'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 ATS, 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 CP/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 ATS, 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 ATS or its affiliates and used by the Relying Party, this CP/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 CP/CPS and any amendments to the CP/CPS are effective when published to the ATS Repository and remain in effect until replaced with a newer version.

### 9.10.2 Termination

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

### 9.10.3 Effect of termination and survival

ATS will communicate the conditions and effect of this CP/CPS's termination via the ATS 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 CP/CPS terminates.

## 9.11 Individual notices and communications with participants

ATS accepts notices related to this CP/CPS at the locations specified in Section 1.5.2 of this CP/CPS. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from ATS. 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 Section 1.5.2 of this CP/CPS using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested. ATS may allow other forms of notice in its Subscriber Agreements.

## 9.12 Amendments

### 9.12.1 Procedure for amendment

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

### 9.12.2 Notification mechanism and period

ATS posts CP/CPS revisions to its Repository. ATS does not guarantee or set a notice-and-comment period and may make changes to this CP/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 CP/CPS.

### 9.12.3 Circumstances under which OID must be changed

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

## 9.13 Dispute resolution provisions

Parties are required to notify ATS and attempt to resolve disputes directly with ATS 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 CP/CPS and all proceedings related to ATS 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 CP/CPS or any ATS product or service. ATS 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 CP/CPS.

## 9.15 Compliance with applicable law

This CP/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

ATS contractually obligates each RA to comply with this CP/CPS and applicable industry guidelines. ATS 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 CP/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 CP/CPS may not assign their rights or obligations without the prior written consent of ATS. Unless specified otherwise in a contract with a party, ATS does not provide notice of assignment.

### 9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/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)

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

### 9.16.5 Force Majeure

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

## 9.17 Other provisions

No stipulation.