amazon trust services

Certificate Policy / Certification Practice Statement

Version 2.2

Contents

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. By design, this CP/CPS closely follows the CA/Browser Forum ("CABF") Guidelines and Requirements and only deviates when an Application Software Supplier has requirements that are stricter than those published by the CABF.

This CP/CPS also includes the principles and criteria that CAs are required to follow according to the latest version of the WebTrust Service Principles and Criteria for Certification Authorities.

CAs following this CP/CPS may have practices which exceed the minimum requirements set forth by these policies. CAs may also describe practices that cover topics for which there is no stipulation in this CP/CPS.

ATS conforms to the current version of the guidelines adopted by the CABF when issuing publicly trusted certificates, including:

- The TLS Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates ("TLS BRs"),
- The Guidelines for Extended Validation Certificates ("EV Guidelines"),
- Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates ("CSBRs"), and
- The Network and Certificate System Security Requirements ("NCSSRs")

Each of these requirements are published at https://www.cabforum.org. If any inconsistency exists between this CP/CPS and the TLS BRs, EV Guidelines, CSBRs, and/or the NCSSRs then the associated requirement or guideline document shall take precedence.

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**
ATS Certificate Policy and Certification Practice Statement	Public	ATS Repository
Subscriber Agreement	Public	ATS Repository
Terms of Use	Public	ATS Repository
ATS Privacy Policy Public https://aws.amazon.com/privacy/	Public	
CA Procedure Documents	Confidential	Presented to auditors accordingly

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

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 Root CA 1	RSA, n has 2048-bits e=65537	fbe3018031f9586b cbf41727e417b7d1 c45c2f47f93be372 a17b96b50757d5a2	May 26 00:00:00 2015 GMT to Jan 17 00:00:00 2038 GMT
C=US O=Amazon CN=Amazon Root CA 2	RSA, n has 4096-bits e=65537	7f4296fc5b6a4e3b 35d3c369623e364a b1af381d8fa71215 33c9d6c633ea2461	May 26 00:00:00 2015 GMT to May 26 00:00:00 2040 GMT
C=US O=Amazon CN=Amazon Root CA 3	EC, NIST P-256 curve	36abc32656acfc64 5c61b71613c4bf21 c787f5cabbee4834 8d58597803d7abc9	May 26 00:00:00 2015 GMT to May 26 00:00:00 2040 GMT
C=US O=Amazon CN=Amazon Root CA 4	EC, NIST P-384 curve	f7ecded5c66047d2 8ed6466b543c40e0 743abe81d109254d cf845d4c2c7853c5	May 26 00:00:00 2015 GMT to May 26 00:00:00 2040 GMT
C=US ST=Arizona L=Scottsdale O=Starfield Technologies,Inc. CN=Starfield Services Root Certificate Authority - G2	RSA, n has 2048-bits e=65537	2b071c59a0a0ae76b0ead b2bad23bad4580b69c360 1b630c2eaf0613afa83f92	Sep 1 00:00:00 2009 GMT to Dec 31 23:59:59 2037 GMT
C = DE O = Amazon CN = Amazon RSA 2048 Root EU M1	RSA, n has 2048-bits e=65537	8d935558e6a3c89633014 8ffdf6a1ac0a5bfba1ab44 545135a3b376c9a1a308d	Nov 14 12:45:15 2024 GMT to Nov 14 12:45:15 2042 GMT
C = DE O = Amazon CN = Amazon ECDSA 256 Root EU M1	EC, NIST P-256 curve	9565907725464be0bff44 b1232f85ee862a9a0d99d b971ba20344aaf41431d5 8	Nov 14 12:45:51 2024 GMT to Nov 14 12:45:51 2042 GMT

C = DE O = Amazon CN = Amazon ECDSA 384 Root EU M1	EC, NIST P-384 curve	798fe10957e8c5a087420 1caf09d5ef4b2e2412c47b f991949566cb542d3af3f	Nov 14 12:46:12 2024 GMT to Nov 14 12:46:12 2042 GMT

Effective June 10, 2015, the *Starfield Services Root Certificate Authority - G2* certification authority operates under this CP/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 ATS CP/CPS. It was approved for publication by the ATS Policy Management Authority ("APPMA") and is made available at https://www.amazontrust.com/repository/. The following revisions were made to the original document:

Date	Changes	Version
Jul 23, 2025	Combined the CP and CPS into a single document and re-versioned. Prior versions can be found at https://www.amazontrust.com/repository/ Annual review and updates.	2.0
Oct 20, 2025	Added language to clarify key validity, MPIC, and new domains verified when performing CAA lookups. References, definitions, and acronyms updated.	2.1
Nov 27, 2025	Updated section 5.7.1 to include statement about ATS's Mass Revocation Plan Minor grammatical updates	2.2

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, revoking a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. The ATS CA is managed by the APPMA, composed of members of ATS management, legal, and technical staff appointed by ATS senior executive(s). The APPMA has responsibility for the review and approval of this CP/CPS and overseeing the governance of CA practices for compliance with applicable requirements.

General information about ATS products and services is available at www.amazon.com.

1.3.2 Registration authorities

ATS 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. ATS 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/CPS will be performed.

1.3.3 Subscribers

See definition of "Subscriber" in Section 1.6.1 of this document.

Subscribers use ATS 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

See definition of "Relying Party" in Section 1.6.1 of this document.

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 ATS CAs as trust anchors in other PKI communities, CMAs, RSPs, CSAs and TSAs.

If a CA subcontracts CMA, RSP, CSA, TSA, or other functions, the CA ensures that compliance with the CP/CPS 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

1.4.1 Appropriate certificate uses

Certificates issued pursuant to this CP/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 CP/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 was issued.

Certificates issued under this CP/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 CP/CPS 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
+1 206 266 1000

Web: www.amazontrust.com
Email for policy questions: appma[@]amazon.com

Contact information for Certificate Problem Reports can be found at:
https://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

The Definitions found in the CABF's NCSSRs are incorporated by reference as if fully set forth herein.

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.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant:

i. who signs and submits, or approves a certificate request on behalf of the Applicant, and/or
ii. who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or
iii. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

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

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

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

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

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.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

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.

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."

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: 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: 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 Practice Statement: 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.

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

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.

DNS CAA Email Contact: The email address defined in Appendix A.1.1.

DNS CAA Phone Contact: The phone number defined in Appendix A.1.2.

DNS TXT Record Email Contact: The email address defined in Appendix A.2.1.

DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

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

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

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

i. the Internet Corporation for Assigned Names and Numbers (ICANN),

ii. a national Domain Name authority/registry, or
iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

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

Fully-Qualified Domain Name: 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.).

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

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

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

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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.

LDH Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

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

Linting: A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

Multi-Perspective Issuance Corroboration: 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.

Non-Reserved LDH Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '--' in the third and fourth positions."

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

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

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.

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

Parent Company: A company that Controls a Subsidiary Company.

Pending Prohibition: The use of a behavior described with this label is highly discouraged, as it is planned to be deprecated and will likely be designated as MUST NOT in the future.

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: 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.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

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.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

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

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

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

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

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

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Baseline Requirements found in this document.

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries:

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

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.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

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.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name or an IP Address listed in the subjectAltName extension or the Subject commonName field.

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

Subscriber: 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.

Test Certificate: This term is no longer used in these Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

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

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

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.

XN-Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix "xn--" (case independent), but otherwise conform to the rules for LDH labels."

1.6.2 Acronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name

CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VoIP	Voice Over Internet Protocol

1.6.3 References

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

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

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

FIPS 140-3, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, March 22, 2019.

FIPS 186-5, Federal Information Processing Standards Publication - Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology, February 2023.

ISO 21188:2018, Public key infrastructure for financial services – Practices and policy framework.

Network and Certificate System Security Requirements, Version 1.7, available at https://cabforum.org/network-security-requirements/

NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf.

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

RFC3492, Request for Comments: 3492, Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA). A. Costello. March 2003.

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

RFC3912, Request for Comments: 3912, WHOIS Protocol Specification. L. Daigle. September 2004.

RFC3986, Request for Comments: 3986, Uniform Resource Identifier (URI): Generic Syntax. T. Berners-Lee, et al. January 2005.

RFC4035, Request for Comments: 4035, Protocol Modifications for the DNS Security Extensions. R. Arends, et al. March 2005.

RFC4509, Request for Comments: 4509, Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs). W. Hardaker. May 2006.

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

RFC5155, Request for Comments: 5155, DNS Security (DNSSEC) Hashed Authenticated Denial of Existence. B. Laurie, et al. March 2008.

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

RFC5702, Request for Comments: 5702, Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC. J. Jansen. October 2009.

RFC5890, Request for Comments: 5890, Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework. J. Klensin. August 2010.

RFC5952, Request for Comments: 5952, A Recommendation for IPv6 Address Text Representation. S. Kawamura, et al. August 2010.

RFC6840, Request for Comments: 6840, Clarifications and Implementation Notes for DNS Security (DNSSEC). S. Weiler, et al. February 2013.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. S. Santesson, et al. June 2013.

RFC6962, Request for Comments: 6962, Certificate Transparency. B. Laurie, et al. June 2013.

RFC7231, Request For Comments: 7231, Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. R. Fielding, et al. June 2014.

RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format. A. Newton, et al. March 2015.

RFC7538, Request For Comments: 7538, The Hypertext Transfer Protocol Status Code 308 (Permanent Redirect). J. Reschke. April 2015.

RFC8499, Request for Comments: 8499, DNS Terminology. P. Hoffman, et al. January 2019.

RFC8659, Request for Comments: 8659, DNS Certification Authority Authorization (CAA) Resource Record. P. Hallam-Baker, et al. November 2019.

RFC8738, Request for Comments: 8738, Automated Certificate Management Environment (ACME) IP Identifier Validation Extension. R.B.Shoemaker, Ed. February 2020.

RFC8954, Request for Comments: 8954, Online Certificate Status Protocol (OCSP) Nonce Extension. M. Sahni, Ed. November 2020.

WebTrust for Certification Authorities, SSL Baseline with Network Security, available at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

WebTrust Principles and Criteria for Certification Authorities – SSL Baseline

X.509, Recommendation ITU-T X.509 (08/2005) | ISO/IEC 9594-8:2005, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

1.6.4 Conventions

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

By convention, this document omits time and timezones when listing effective requirements such as dates. Except when explicitly specified, the associated time with a date shall be 00:00:00 UTC.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ATS makes its Publicly-Trusted 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 CP/CPS. ATS's legal repository is located at https://www.amazontrust.com/repository. ATS 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.

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

2.2 Publication of certification information

ATS 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

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 to the document.

New or updated versions of Subscriber Agreements, or Relying Party representations and warranties (as described in Section 9.6.4) are typically published within seven days after their approval.

CA certificates are published in a repository as soon as possible after issuance, typically within seven days. CRLs are published in accordance with Section 4.9.7 of this policy. ATS may publish new CRLs prior to the scheduled issuance of the next CRL.

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 this CP/CPS.

3.1.2 Need for names to be meaningful

ATS 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

The uniqueness of each subject name in a Certificate is enforced by inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Name uniqueness is not violated when multiple certificates are issued to the same entity.

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 CP/CPS, ATS does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. ATS 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 organizational or individual Applicant. ATS may refuse to issue a Certificate at its sole discretion.

For EV Certificates, ATS takes all verification steps reasonably necessary to satisfy the EV Verification Requirements set forth in the EV Guidelines.

For Code Signing Certificates, ATS takes all verification steps reasonably necessary to satisfy the verification requirements set forth in the CSBRs.

3.2.1 Method to prove possession of private key

ATS 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

ATS confirms the Applicant has control of or right to use Email Addresses by contacting the requested email address and confirming authorization of the Certificate's issuance.

ATS does not use the following methods described in the CABF TLS BRs: 3.2.2.4.1, 3.2.2.4.2, 3.2.2.4.3, 3.2.2.4.5, 3.2.2.4.6, 3.2.2.4.9, 3.2.2.4.10, and 3.2.2.4.11, 3.2.2.4.15.

Prior to issuance of a Subscriber certificate, ATS uses one of the following CABF TLS BR methods to validate control of each requested DNS name:3.2.2.4.4, 3.2.2.4.7 3.2.2.4.8, 3.2.2.4.12, 3.2.2.4.13, 3.2.2.4.14, 3.2.2.4.16, 3.2.2.4.17, 3.2.2.4.18, 3.2.2.4.19, and 3.2.2.4.20. Validations are performed by Primary Network Perspectives and corroborated by at least the minimum quorum of Remote Network Perspectives defined in the CABF TLS BRs effective at the time of validation. All validations are performed in accordance with, and are compliant with, the CABF TLS BRs at the time of validation.

If the Applicant requests an Extended Validation Certificate, then ATS follows the EV Guidelines.

3.2.3 Authentication of individual identity

This section is not applicable since ATS does not issue certificates to individuals.

3.2.4 Non-verified subscriber information

All subscriber information required by the chosen certificate type is verified.

3.2.5 Validation of authority

ATS 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 ATS will not accept any certificate requests that are outside this

specification. A request to limit authorized individuals is not effective until approved by ATS. ATS 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

ATS discloses all Cross-Certified Subordinate CA Certificates that identify the CA as the Subject and are part of a trust relationship recognized by ATS by placing copies of the cross certificate in the Repository.

3.3 Identification and authentication for re-key requests

ATS 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 Section 3.2 of this CP/CPS.

3.3.2 Identification and authentication for re-key after revocation

As per Section 3.2 of this CP/CPS.

3.4 Identification and authentication for revocation request

ATS or an RA authenticates all revocation requests that are at the Subscriber's request. ATS 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 Section 4.9 of this CP/CPS, 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

Any Applicant or an authorized Certificate Requester that is a customer of either (1) ATS Web Services or (2) an authorized reseller of ATS Web Services offerings, may submit certificate requests. Applicants are responsible for the accuracy of any data submitted.

ATS shall only issue EV TLS and Code Signing Certificates to Applicants which meet the requirements specified in the CABF's EV Guidelines and CSBRs, respectively, in addition to the requirements of this CP/CPS.

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 ATS,
- Agreeing to the applicable Subscriber Agreement, and,
- Paying any applicable fees.

ATS obtains any additional documentation it determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, ATS obtains from the Applicant a certificate request in a form prescribed by ATS and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 4.2.1 CP/CPS, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

ATS or an RA (as described in Section 1.3.2 of this CP/CPS) verifies the application information and other information specified in this CP/CPS. As part of this verification, ATS 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 ATS employee, RA, or agent skilled in the language assists in the identification and authentication.

As part of the validation process, ATS checks for CAA records for each requested DNS name and follows the processing instructions found as described in RFC 8659 and Section 3.2.2.8 of the CABF TLS BRs. ATS proceeds in accordance with CAA records if present. Issuance is performed within the TTL of the CAA record, or 8 hours, whichever is greater.

We look for amazon.com, amazontrust.com, awstrust.com, amazonaws.com, amazontrustservices.eu, amazonaws.eu, or amznts.eu in CAA records. We also may accept FQDNs which are subordinate to these names (for example aws.amazon.com).

4.2.2 Approval or rejection of certificate applications

ATS will not issue certificates containing Internal Names or Reserved IP Addresses, as such names cannot be validated according to Section 3.2.2.4 or Section 3.2.2.5.

For Applications for a Subordinate CA where the Subordinate CA will not be controlled by, ATS 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 CABF guidelines
- The CA generated and stores its keys on a HSM that meets the requirements in the CP/CPS
- 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/CPS.
- 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.

ATS will post links to Subordinate CA certificates, CP, CPS, 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

Certificate issuance by the Root CA SHALL require an individual authorized by ATS (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

ATS 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.

Automated pre-issuance linting is incorporated into the issuance workflow for Subscriber certificates. ATS uses up-to-date, industry standard linting tools. Errors discovered during pre-issuance linting will prevent certificate issuance and are logged.

4.3.2 Notification to subscriber by the CA of issuance of certificate

ATS will deliver certificates within a reasonable time after issuance. Generally, ATS 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

ATS 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.

ATS 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

See Section 9.6.3 of this CP/CPS, provisions 2. and 4.

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. ATS 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 ATS are only valid if a Relying Party's reliance was reasonable.

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

1. The digital signature or 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 CP/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

Take into account any other precautions prescribed in this CP/CPS or elsewhere.

4.6 Certificate renewal

ATS 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

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 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

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 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
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
Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. ATS supports Certificate Revocation. Certificate suspension is not used.

4.9.1 Circumstances for revocation
ATS 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.

4.9.1.1 Reasons for Revoking a Subscriber Certificate
ATS may support revocation of Short-lived Subscriber Certificates.

With the exception of Short-lived Subscriber Certificates, ATS will revoke a Certificate within 24 hours and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that ATS revoke the Certificate (CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies ATS that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. ATS obtains evidence that the Subscriber’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

4. ATS is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3(5) (CRLReason #1, keyCompromise);

5. ATS obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

With the exception of Short-lived Subscriber Certificates, ATS may revoke a certificate within 24 hours and will revoke a Certificate within 5 days and use the corresponding CRLReason (see Section 7.2.2) if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 (CRLReason #4, superseded);

2. ATS obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);

3. ATS is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);

4. ATS is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);

5. ATS is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

6. ATS is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);

7. ATS is made aware that the Certificate was not issued in accordance with these Requirements or ATS's CP/CPS (CRLReason #4, superseded);

8. ATS determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);

9. ATS's right to issue Certificates under these Requirements expires or is revoked or terminated, unless ATS has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);

10. Revocation is required by ATS's CP/CPS for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or

11. ATS is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

ATS will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies ATS that the original certificate request was not authorized and does not retroactively grant authorization;

3. ATS obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. ATS obtains evidence that the Certificate was misused;
5. ATS is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. ATS determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. ATS or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. ATS's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless ATS has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by ATS's CP/CPS.

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. ATS 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/CPS. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

4.9.3 Procedure for revocation request

ATS processes a revocation request as follows:

1. ATS logs the identity of entity making the request or problem report and the reason for requesting revocation. ATS may also include its own reasons for revocation in the log.
2. ATS 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, ATS revokes the certificate.
4. For requests from third parties, ATS 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 ATS determines that revocation is appropriate; ATS personnel revoke the certificate and update the CRL.

ATS maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, ATS 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. ATS 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

Within 24 hours after receiving a Certificate Problem Report, ATS will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report. After reviewing the facts and circumstances, ATS will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which ATS will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation will not exceed the time frame set forth in Section 4.9.1.1. The date selected by ATS may consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
5. Relevant legislation.

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)

ATS makes CRLs available via a publicly-accessible HTTP URL (i.e., "published").

Within twenty-four (24) hours of issuing its first Certificate, ATS will generate and publish either:

- a full and complete CRL; OR
- partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL.

When issuing Subscriber Certificates, ATS:

1. Updates and publishes a new CRL at least every:
    - seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"); or
    - four (4) days in all other cases;
2. Updates and publishes a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

When issuing CA Certificates, ATS:

1. Updates and publishes a new CRL at least every twelve (12) months;

2. Updates and publishes a new CRL within twenty-four (24) hours after recording a Certificate as revoked.

ATS will continue issuing CRLs until one of the following is true:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed.

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. 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.

4.9.9 On-line revocation/status checking availability

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

The following applies for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

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

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-line revocation checking requirements

A relying party must confirm the validity of a certificate prior to relying on the certificate. The following applies for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

OCSP responders operated by ATS support the HTTP GET method, as described in RFC 6960 and/or RFC 5019. ATS may process the Nonce extension (`1.3.6.1.5.5.7.48.1.2`) in accordance with RFC 8954.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

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

For the status of Subordinate CA Certificates:

1. ATS will update information provided via an Online Certificate Status Protocol at least every twelve months; and
2. within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder will not respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.2.3 or Section 7.1.2.5, the responder will not respond with a "good" status for such requests.

The OCSP responder may provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962].

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by ATS, using any current or previous key associated with that ATS subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by
    a. ATS; or
    b. a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with ATS; or
3. "unused" if neither of the previous conditions are met.

4.9.11 Other forms of revocation advertisements available

ATS allows, but does not require, OCSP stapling.

4.9.12 Special requirements re key compromise

See Section 4.9.1.

Contact information for reporting private key compromise can be found at:
https://www.ATStrust.com/repository/

Proof of key compromise should be submitted in either of the following formats:

- A CSR signed by the compromised private key with the Common Name "Proof of Key Compromise for Amazon"; or
- The private key itself.

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

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 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

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

ATS maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

ATS maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

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

5.1.3 Power and air conditioning

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

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 the CA.

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

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 ATS'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 ATS, 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.

Amazon PKI Policy Management Authority Member

> The APPMA is responsible for approving this CP/CPS and certain other documents related to CAs in ATS. 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

> ATS Managers are responsible for PKI Operations and CA documents, including the Certificate Policy and Certification Practice Statement. 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 ATS, an Issuer CA, or RA is operating in accordance with this CP/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

ATS 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 APPMA 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 ATS operations and ensures compliance with this CP/CPS. ATS personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. The APPMA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP/CPS.

5.3.2 Background check procedures

ATS 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. ATS 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 performed 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

ATS 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 ATS's validation and verification policies and procedures. ATS documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

5.3.4 Retraining frequency and requirements

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

ATS 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

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 in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP/CPS, EV Guidelines, 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 log files are generated for all events relating to the security and services of the CA. Where possible, the security audit logs are automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism are used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

ATS 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.

ATS records at least the following events:

1. CA certificate and key lifecycle events, including:
    1. Key generation, backup, storage, recovery, archival, and destruction;
    2. Certificate requests, renewal, and re-key requests, and revocation;

3. Approval and rejection of certificate requests;
4. Cryptographic device lifecycle management events;
5. Generation of Certificate Revocation Lists
6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

2. Subscriber Certificate lifecycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    3. Approval and rejection of certificate requests;
    4. Issuance of Certificates;
    5. Generation of Certificate Revocation Lists and;
    6. Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Security profile changes;
    4. Installation, update and removal of software on a Certificate System;
    5. System crashes, hardware failures, and other anomalies;
    6. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    7. Entries to and exits from the CA facility.

5.4.1.1 Router and firewall activities logs

ATS logs router and firewall activities necessary to meet the requirements of Section 5.4.1, Subsection 3.6 and minimally includes:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of processing log

CA management reviews logs in the audit log repository as needed.

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

ATS 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

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

5.5.1 Types of records archived

ATS archives both application and system data. ATS may archive the following information:

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

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 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. ATS maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If ATS needs to transfer any media to a different archive site or equipment, ATS 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

ATS 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

ATS 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 ATS.

5.5.7 Procedures to obtain and verify archive information

ATS's primary and backup archives are only accessible by authorized ATS personnel.

ATS does not release archives in their entirety, except as required by law.

ATS may require compensation and fees for any costs incurred in accessing or retrieving any requested archival data.

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, ATS 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 ATS has cross-certified another CA that is in the process of a key rollover, ATS 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

5.7.1.1 Incident Response and Disaster Recovery Plans

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST include:

1. The conditions for activating the plan,
2. Emergency procedures,

3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and

Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.1.2 Mass Revocation Plans

ATS maintains a comprehensive mass revocation plan that is tested on an annual basis. Findings and observations from the annual test are reviewed and incorporated into the plan for continuous improvement.

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.

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

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:

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 ATS's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, ATS 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

Make other necessary arrangements that are in accordance with this CP/CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

For CA Key Pairs that are either

i. used as a CA Key Pair for a Root Certificate, or

ii. used as a CA Key Pair for a Subordinate CA Certificate, where the Subordinate CA is not the operator of the Root CA or an Affiliate of the Root CA,

ATS will:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, ATS may:

1. prepare and follow a Key Generation Script, and
2. have a Qualified Auditor witness the CA Key Pair generation process or record a video of the entire CA Key Pair generation process.

In all cases, ATS will generate the CA Key Pair in a physically secured environment as described in this CP/CPS, and:;

1. generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
2. generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in this CP/CPS;
3. log its CA Key Pair generation activities; and

4. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP/CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

Subscriber key pairs are generated by the Subscriber. ATS will reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. ATS is aware of a demonstrated or proven method that exposes the Applicant's Private Key to compromise;
4. ATS has previously been notified that the Applicant's Private Key has suffered a Key Compromise using ATS's procedure for revocation request as described in Section 4.9.3 and Section 4.9.12;
5. The Public Key corresponds to an industry-demonstrated weak Private Key. For requests submitted on or after November 15, 2024, at least the following precautions will be implemented:
    1. In the case of Debian weak keys vulnerability (https://wiki.debian.org/SSLkeys), ATS will reject all keys found at https://github.com/cabforum/Debian-weak-keys/ for each key type (e.g. RSA, ECDSA) and size listed in the repository. For all other keys meeting the requirements of Section 6.1.5, with the exception of RSA key sizes greater than 8192 bits, ATS will reject Debian weak keys.
    2. In the case of ROCA vulnerability, ATS will reject keys identified by the tools available at https://github.com/crocs-muni/roca or equivalent.
    3. In the case of Close Primes vulnerability (https://fermatattack.secvuln.info/), ATS will reject weak keys which can be factored within 100 rounds using Fermat's factorization method.

If the Subscriber Certificate will contain an extKeyUsage extension containing either the values id-kp-serverAuth [RFC5280] or anyExtendedKeyUsage [RFC5280], ATS will not generate a Key Pair on behalf of a Subscriber, and will not accept a certificate request using a Key Pair previously generated by ATS.

6.1.2 Private key delivery to subscriber

ATS 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 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 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 ATS certificates and all application software providers are permitted to redistribute ATS root anchors.

ATS 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 ATS self- signed CA certificates from the ATS web site.

6.1.5 Key sizes

For RSA key pairs ATS will:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8.

For ECDSA key pairs, ATS will:

- Ensure that the key represents a valid point on the NIST P-256, NIST P-384 or NIST P-521 elliptic curve.

6.1.6 Public key parameters generation and quality checking

ATS 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.

RSA: ATS confirms that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent is in the range between 2^16 + 1 and 2^256 - 1. The modulus also has the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89]

ECDSA: ATS confirms the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC 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)

ATS includes Key Usage and Extended Key Usage fields in certificates as defined in the applicable certificate profile. Private Keys corresponding to Root Certificates will not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

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 140-1 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

ATS 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

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 Private Keys are generated and stored inside cryptographic modules which meet the requirements of Section 6.2.1 of this CP/CPS.

6.2.8 Method of activating private key

ATS 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

ATS 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. ATS never leaves its HSM devices in an active unlocked or unattended state.

6.2.10 Method of destroying private key

ATS personnel, acting in trusted roles, 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. Certificates signed by Root CA keys have a validity period that terminates on or before the end of the validity period of the corresponding Root Certificate.

Subscriber Certificates will not have a Validity Period greater than 398 days.

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

ATS systems maintaining CA software and data files are secure from unauthorized access.

ATS enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

ATS has established a security framework which covers and governs the technical aspects of its computer security.

6.6 Life cycle technical controls

6.6.1 System development controls

ATS 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. ATS 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 are 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 ATS 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 ATS operations are scanned for malicious code on first use and periodically thereafter.

6.6.2 Security management controls

ATS has mechanisms in place to control and monitor the security-related configurations of its CA systems.

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 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.

All CA and RA systems must be protected in accordance with the NCSSRs.

Vulnerability remediation timelines are governed by severity according to the following Service Level Agreements (SLAs):

- Emergent: This is an immediate investigation response 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

ATS Certificates conform to RFC 5280, including fields and extensions not specifically mentioned. ATS also meets the technical requirements set forth in CABF TLS BRs EV Guidelines, and CSBRs, where applicable.

7.1.1 Version number(s)

All certificates are X.509 version 3 certificates.

7.1.2 Certificate extensions

All certificate extensions comply with RFC5280 and applicable CABF requirements.

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 and with Section 7.1.4 of the CABF TLS BRs.

7.1.5 Name constraints

Not applicable.

7.1.6 Certificate policy object identifier

Certificates that are issued under ATS and are compliant with the CABF TLS BRs contain the policy object identifier 2.23.140.1.2.1. The object identifier 1.3.187.1 may be included in their policy list.

Certificates that are issued under ATS and are complaint with the CABF EV Guidelines contain the policy object identifier 2.23.140.1.2.3. The object identifier 1.3.187.1.1 may be included in their policy list.

Certificates that are issued under ATS and are complaint with the CSBRs contain the policy object identifier 2.23.140.1.3. The object identifier 1.3.187.1.1 may be included in their 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

ATS CRL profiles conform to RFC 5280, including fields and extensions not specifically mentioned. ATS also meets the technical requirements set forth in CABF TLS BRs and EV Guidelines, where applicable.

7.2.1 Version number(s)

ATS issues version 2 CRLs.

7.2.2 CRL and CRL entry extensions

CRL reasonCodes are required for CRL entries applicable to CA certificates.

CRL reasonCodes are included in the reasonCode extension of the CRL entry corresponding to an end-entity certificate unless the CRLReason is "unspecified (0)". Only the following CRLReasons may be present in the CRL reasonCode extension for end-entity certifificates:

CRLReasons

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
unspecified	0	Represented by the omission of a reasonCode. MUST be omitted if the CRL entry is for a Certificate not technically capable of causing issuance unless the CRL

RFC 5280 reasonCode	RFC 5280 reasonCode value	Description
		entry is for a Subscriber Certificate subject to these Requirements revoked prior to July 15, 2023.
keyCompromise	1	Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.
affiliationChanged	3	Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.
superseded	4	Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with these Baseline Requirements or the CA's CP or CPS.
cessationOfOperation	5	Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.
privilegeWithdrawn	9	Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

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

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

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 described in Section 8.2 of the TLS BRs, 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

If an audit reports material noncompliance with applicable law, this CP/CPS, or any other contractual obligations related to ATS, then (1) the auditor will document the discrepancy, (2) the auditor will promptly notify ATS, and (3) ATS will develop a plan to cure the noncompliance. ATS 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 noncompliance, 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, ATS submits a report of its audit compliance to various parties, such as Mozilla, Microsoft, CA licensing bodies, etc. ATS is not required to make publicly available any general audit finding that does not impact the overall audit opinion.

8.7 Self-Audits

During the period in which ATS issues Certificates, ATS will monitor adherence to its CP/CPS and these Requirements and strictly control its service quality by performing self-audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.4, ATS will control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by ATS perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. ATS will review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

ATS will internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

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

ATS does not charge Subscribers for revocation.

9.1.5 Refund policy

ATS refunds customers for erroneous charges.

9.2 Financial responsibility

9.2.1 Insurance coverage

- ATS maintains general liability insurance coverage with policy limits of at least two million US dollars in coverage.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

ATS maintains insurance or self-insures in accordance with Section 9.2.1 of this CP/CPS.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following information is considered confidential information of ATS 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 ATS as private information in accordance with 9.3 Confidentiality of Business Information;
6. Audit logs and archive records; and

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 CP/CPS).

9.3.2 Information not within the scope of confidential information

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

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 the certificates, trademarks used in providing the services, and this CP/CPS. Certificate and revocation information are the property of ATS. ATS 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 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 in the TLS BRs, and
4. ATS will maintain a repository of public information on its website.

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

This foregoing warranty is limited solely to ATS compliance with the EV Guidelines (e.g., ATS 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 ATS CP/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 CP/CPS.

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

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, 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 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. IN ANY CASE, OUR AND OUR AFFILIATES' AND LICENSORS' AGGREGATE LIABILITY IN CONNECTION WITH THIS CP/CPS AND ALL CERTIFICATES ISSUED HEREUNDER, IS LIMITED TO $500; PROVIDED, HOWEVER, THAT FOR ANY EV CERTIFICATE ISSUED UNDER THIS CP/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

ATS 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 ATS 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 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.

APPENDIX A – CAA Contact Tag

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

A.1 CAA Methods

A.1.1 CAA contactemail Property

SYNTAX: contactemail <rfc6532emailaddress>

The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532, Section 3.2, with no additional padding or structure, or it cannot be used.

The following is an example where the holder of the domain specified the contact property using an email address.

DNS Zone $ORIGIN example.com. CAA 0 contactemail "domainowner@example.com"

The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

A.1.2 CAA contactphone Property

SYNTAX: contactphone <rfc3966 Global Number>

The CAA contactphone property takes a phone number as its parameter. The entire parameter value MUST be a valid Global Number as defined in RFC 3966, Section 5.1.4, or it cannot be used. Global Numbers MUST have a preceding + and a country code and MAY contain visual separators.

The following is an example where the holder of the domain specified the contact property using a phone number.

DNS Zone $ORIGIN example.com. CAA 0 contactphone "+1 (555) 123-4567"

The contactphone property MAY be critical if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

A.2 DNS TXT Methods

A.2.1 DNS TXT Record Email Contact

The DNS TXT record MUST be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532, Section 3.2, with no additional padding or structure, or it cannot be used.

A.2.2 DNS TXT Record Phone Contact

The DNS TXT record MUST be placed on the "_validation-contactphone" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid Global Number as defined in RFC 3966, Section 5.1.4, or it cannot be used.

APPENDIX B – Issuance of Certificates for Onion Domain Names

This appendix defines permissible verification procedures for including one or more Onion Domain Names in a Certificate.

1. The Domain Name MUST contain at least two Domain Labels, where the rightmost Domain Label is "onion", and the Domain Label immediately preceding the rightmost "onion" Domain Label is a valid Version 3 Onion Address, as defined in Section 6 of the Tor Rendezvous Specification - Version 3 located at https://spec.torproject.org/rend-spec-v3.
2. ATS will verify the Applicant's control over the Onion Domain Name using at least one of the methods listed below:
    a. ATS may verify the Applicant's control over the .onion service by using one of the following methods from Section 3.2.2.4:
        i. Section 3.2.2.4.18 - Agreed-Upon Change to Website v2
        ii. Section 3.2.2.4.19 - Agreed-Upon Change to Website - ACME
        iii. Section 3.2.2.4.20 - TLS Using ALPN

    When these methods are used to verify the Applicant's control over the .onion service, ATS will use Tor protocol to establish a connection to the .onion hidden service. ATS will not delegate or rely on a third-party to establish the connection, such as by using Tor2Web.

    Note: This section does not override or supersede any provisions specified within the respective methods. ATS will only use a method if it is still permitted within that section and will not issue Wildcard Certificates or use it as an Authorization Domain Name, except as specified by that method.

    b. ATS may verify the Applicant's control over the .onion service by having the Applicant provide a Certificate Request signed using the .onion service's private key if the Attributes section of the certificationRequestInfo contains:
        i. A caSigningNonce attribute that contains a Random Value that is generated by ATS; and
        ii. An applicantSigningNonce attribute that contains a single value. ATS will recommend to Applicants that the applicantSigningNonce value should contain at least 64 bits of entropy.

    The signing nonce attributes have the following format:

```
cabf OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) international-
organizations(23) ca-browser-forum(140) }

caSigningNonce ATTRIBUTE ::= {

WITH SYNTAX                    OCTET STRING

EQUALITY MATCHING RULE  octetStringMatch

SINGLE VALUE                   TRUE

ID                        { cabf-caSigningNonce }

}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {
```

```
WITH SYNTAX                    OCTET STRING
EQUALITY MATCHING RULE  octetStringMatch
SINGLE VALUE                   TRUE
ID                        { cabf-applicantSigningNonce }
}
cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CP/CPS MAY specify a shorter validity period for Random Values.

Once the FQDN has been validated using this method, ATS may also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3. When a Certificate includes an Onion Domain Name, the Domain Name shall not be considered an Internal Name provided that the Certificate was issued in compliance with this Appendix B.