

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

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

WebTrust for Certification Authorities Version 2.0, available at <http://www.webtrust.org/homepage-documents/item27839.aspx>.

X.509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

4. 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 issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

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 and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of 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 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.

CAA Record: [The Certification Authority Authorization \(CAA\) DNS Resource Record of RFC 6844 \(http://tools.ietf.org/html/rfc6844\) that allows a DNS domain name holder to specify the Certification Authorities \(CAs\) authorized to issue certificates for that domain. Publication of a CAA Resource Record allows public Certification Authorities to implement additional controls to reduce the risk of unintended certificate mis-issue.](http://tools.ietf.org/html/rfc6844)

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

5. Abbreviations and Acronyms

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

6. Conventions

Terms not otherwise defined in these Requirements shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.

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.

6. **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;
7. **Status:** That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

7.2 By the Applicant

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 of these Requirements, for the benefit of the CA and the Certificate Beneficiaries.

8. Community and Applicability

8.1 Compliance

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in Section 17; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

If a court or government body with jurisdiction over the activities covered by these Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

8.2 Certificate Policies

8.2.1 Implementation

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

8.2.2 Disclosure

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 17.1). The disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647. Effective as of [insert date that is six months from Ballot 125 adoption], section 4.2 of a CA's Certificate Policy and/or Certification Practice Statement (section 4.1 for CA's still conforming to RFC 2527) shall disclose: (1) whether the CA reviews CAA Records, and if so, (2) the CA's policy or practice on processing CAA Records and comparing them with proposed Domain Names for the Common Name field or Subject Alternative Name fields of certificates applications, and (3) any actions taken as result of such comparison.