1. INTRODUCTION

1.1. OVERVIEW

This CP describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by relying-party Application Software Suppliers.

Notice to Readers

The CP for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue Publicly Trusted Certificates. This document serves two purposes: to specify Baseline Requirements and to provide guidance and requirements for what a CA should include in its CPS. Except where explicitly stated otherwise, these Requirements apply only to relevant events that occur on or after the Effective Date.

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted Certificates. In accordance with RFC 3647 and to facilitate a comparison of other certificate policies and CPSs (e.g. for policy mapping), this CP includes all sections of the RFC 3647 framework. However, rather than beginning with a “no stipulation” comment in all empty sections, the CA/Browser Forum is leaving such sections initially blank until a decision of “no stipulation” is made. The CA/Browser Forum may update these Requirements from time to time, in order to address both existing and emerging threats to online security. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

These Requirements only address Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

These Requirements are applicable to all Certification Authorities within a chain of trust. They are to be flowed down from the Root Certification Authority through successive Subordinate Certification Authorities.

1.2. DOCUMENT NAME AND IDENTIFICATION

This certificate policy (CP) contains the requirements for the issuance and management of publicly-trusted SSL certificates, as adopted by the CA/Browser Forum.

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with this CP (OID arc 2.23.140.1.2) as follows:

\{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)\} (2.23.140.1.2.1); and

\{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)\} (2.23.140.1.2.2).

1.2.1. Revisions

<table>
<thead>
<tr>
<th>Ver.</th>
<th>Ballot</th>
<th>Description</th>
<th>Adopted</th>
<th>Effective*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>62</td>
<td>Version 1.0 of the Baseline Requirements Adopted</td>
<td>22-Nov-11</td>
<td>01-Jul-12</td>
</tr>
<tr>
<td>1.0.1</td>
<td>71</td>
<td>Revised Auditor Qualifications</td>
<td>08-May-12</td>
<td>01-Jan-13</td>
</tr>
</tbody>
</table>
1.3.5. Other Participants
Other groups that have participated in the development of these Requirements include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses
The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. These Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

1.4.2. Prohibited Certificate Uses
No stipulation.

1.5. POLICY ADMINISTRATION

1.5.1. Organization administering the document
This Certificate Policy for Baseline Requirements for the Issuance and Management of Publicly- Trusted Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Certificates. This CP may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of this CP is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at questions@cabforum.org. The Forum members value all input, regardless of source, and will seriously consider all such input.

1.5.2. Contact person
Contact information for the CA/Browser Forum is available here: https://cabforum.org/leadership/

In this section of a CA's CPS, the CA shall provide a link to a web page or an email address for contacting the person or persons responsible for operation of the CA.

1.5.3. Person determining CPS suitability for the policy
No stipulation.

1.5.4. CPS approval procedures
No stipulation.

1.6. DEFINITIONS AND ACRONYMS

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

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the
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 8.1). 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 15 April 2015, section 4.2 of a CA’s Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state whether the CA reviews CAA Records, and if so, the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA SHALL log all actions taken, if any, consistent with its processing practice.

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):

[Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

2.3. **TIME OR FREQUENCY OF PUBLICATION**

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.

2.4. **ACCESS CONTROLS ON REPOSITORIES**

The CA shall make its Repository public available in a read-only manner.