8 Community and Applicability

8.1 Issuance of EV Certificates

The CA MAY issue EV Certificates, provided that the CA and its Root CA satisfy the requirements in these Guidelines and the Baseline Requirements.

If a court or government body with jurisdiction over the activities covered by these Guidelines 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 Guidelines accordingly.

8.2 EV Policies

8.2.1 Implementation

Each CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Certificate practices, policies and procedures, such as a Certification Practice Statement (CPS) and Certificate Policy (CP) that:

(A) Implement the requirements of these Guidelines as they are revised from time-to-time;

(B) Implement the requirements of (i) the then-current WebTrust Program for CAs, and ~~(ii)~~ the then-current WebTrust EV Program or (ii) the then-current ETSI TS 102 042 including ~~V2.1.1~~EVCP or EVCP+ policy requirements; and

(C) Specify the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity.

8.2.2 Disclosure

Each CA MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices as required by both WebTrust for CAs and ETSI TS 102 042 ~~V2.1.1~~. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Comply with Recommendations

Each CA SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective EV Policies, using a clause such as the following (which must include a link to the official version of these Guidelines):

> [Name of CA] conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

In addition, the CA MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts with Subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

8.4 Insurance

Each CA SHALL maintain the following insurance related to their respective performance and obligations under these Guidelines:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and

The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

14.2.2 Enterprise RAs

The CA MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize the CA to issue additional EV Certificates at third and higher domain levels that are contained within the domain of the original EV Certificate (also known as an Enterprise EV Certificate). In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

(1) An Enterprise RA SHALL NOT authorize the CA to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;

(2) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with these Guidelines;

(3) The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;

(4) The Final Cross-Correlation and Due Diligence requirements of Section 11.12 of these Guidelines MAY be performed by a single person representing the Enterprise RA; and

(5) The audit requirements of Section 17.1 of these Guidelines SHALL apply to the Enterprise RA, except in the case where the CA maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

14.2.3 Guidelines Compliance Obligation

In all cases, the CA MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in these Guidelines and to perform them as required of the CA itself. The CA SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

14.2.4 Allocation of Liability

As specified in Section 14.2.4 of the Baseline Requirements.

15 Data Records

As specified in Section 15 of the Baseline Requirements.

16 Data Security

As specified in Section 16 of the Baseline Requirements. In addition, systems used to process and approve EV Certificate Requests MUST require actions by at least two trusted persons before creating an EV Certificate.

17 Audit

17.1 Eligible Audit Schemes

A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:

(i) WebTrust Program for Certification Authorities ~~audit~~ and WebTrust EV Program audit, or

(ii) ETSI TS 102 042 ~~v2.1.1~~ audit including EVCP or EVCP+ policy requirements.

If the CA is a Government Entity, an audit of the CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly

certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.

EV audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by the CA or delegated to an RA or subcontractor.

17.2 Audit Period

CAs issuing EV Certificates MUST undergo an annual audit that meets the criteria of Section 17.1.

17.3 Audit Record

CAs SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by its auditor.

17.4 Pre-Issuance Readiness Audit

(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

(2) If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042~~ V2.1.1~~ including EVCP or EVCP+ policy requirements.

(3) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete either: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, or (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or an ETSI TS 102 042 ~~V2.1.1.~~ audit including EVCP or EVCP+ policy requirements.

The CA MUST complete any required point-in-time readiness assessment no earlier than twelve (12) months prior to issuing an EV Certificate. The CA MUST undergo a complete audit under such scheme within ninety (90) days of issuing the first EV Certificate.

17.5 Regular Self Audits

During the period in which it issues EV Certificates, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 of these Guidelines is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

17.6 Auditor Qualification

A Qualified Auditor (as defined in Section 17.6 of the Baseline Requirements) MUST perform the CA's audit.

17.7 Root CA Key Pair Generation

All requirements in Section 17.7 of the Baseline Requirements apply equally to EV Certificates. However, for Root CA Key Pairs generated after the release of these Guidelines, the Root CA Key Pair generation ceremony MUST be witnessed by the CA's Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. The Qualified Auditor MUST then issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

(1) Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement;

(2) Included appropriate detail in its Root Key Generation Script;