Guidelines Version 1.1 Errata

1. QGIS for place of business address

Replace Section 16a with the following text, effective 6 May 2008.

(a) Address of Applicant's Place of Business

(1) Verification Requirements To verify Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by Applicant is an address where Applicant or a Parent/Subsidiary Company conducts business operations (e.g., not a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for an agent of the Organization), and is the address of Applicant's Place of Business.

(2) Acceptable Methods of Verification To verify the address of Applicant's Place of Business:

(A) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration:

(1) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Section (14) to verify legal existence:

(1) For Applicants listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST confirm that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant or a Parent/Subsidiary Company by reference to such Qualified Independent Information Sources or a Qualified Governmental Tax Information Source, and MAY rely on Applicant's representation that such address is its Place of Business;

(2) For Applicants who are not listed at the same Place of Business address in the current version of either at least one Qualified Independent Information Source or a Qualified Governmental Tax Information Source, the CA MUST confirm that the address provided by Applicant in the EV Certificate Request is in fact Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:
(a) Verify that Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.);
(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location;
(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies

Applicant;
(d) Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.); and
(e) Include one or more photos of (i) the exterior of the site (showing signage indicating Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace

(3) For all Applicants, the CA MAY alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.

(4) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in Applicant's Jurisdiction.

(2) For Applicants whose Place of Business is in the same country as Applicant's Jurisdiction of Incorporation or Registration and where the Qualified Government Information Source used in Section (14) to verify legal existence contains a business address for the Applicant, the CA MAY rely on the Address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company address as listed in the EV Certificate Request, and MAY rely on Applicant's representation that such address is its Place of Business.

(B) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, the CA MUST rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there.

2. Scope

Replace the following paragraph from Section 1.(b), effective 18 June 2008.

"This version of the Guidelines addresses only requirements for EV Certificates intended to be used for server-authentication SSL/TLS on the Internet. Similar requirements for client-authentication SSL/TLS, S/MIME, code-signing, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions."

With:

"This version of the Guidelines addresses only requirements for EV Certificates intended to be used for SSL/TLS authentication on the Internet and code-signing. Similar requirements for S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions."

3. Allowed EKU values

Add the following clause to Appendix B, section 3, effective 18 June 2008.

"(e) extKeyUsage

Either the value id-kp-serverAuth [RFC3280] or id-kp-clientAuth [RFC3280] or both values MUST be present. Other values SHOULD NOT be present."

4. RFC5280

Effective 11 July 2008, replace 'RFC3280' with 'RFC5280' throughout the document.

5. Certificate renewal (same CA)

Effective 25 July 2008.

5.1 Replace this paragraph from Section 8.

8. Maximum Validity Period

(b) For Validated Data the age of validated data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:
(1) Legal existence and identity – one year;
(2) Assumed name – one year;
(3) Address of Place of Business – one year, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
(4) Telephone number for Place of Business – one year;
(5) Bank account verification – one year;
(6) Domain name – one year;
(7) Identity and authority of Certificate Approver – one year, unless a contract is in place between the CA and Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

With

8. Maximum Validity Period

(b) For Validated Data the age of validated data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:
(1) Legal existence and identity – thirteen months;
(2) Assumed name – thirteen months;

(3) Address of Place of Business – thirteen months, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source, even where a site visit was originally required;
(4) Telephone number for Place of Business – thirteen months;
(5) Bank account verification – thirteen months;
(6) Domain name – thirteen months;
(7) Identity and authority of Certificate Approver – thirteen months, unless a contract is in place between the CA and Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

5.2 Add the following paragraph as Section 22(d)(3)

22(d)(3) - The CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The CA MAY rely on this verified contact information for future correspondence with the Confirming Person if:

1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias,

2. The Confirming Person's telephone/fax number is verified by the CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

5.3 Replace this paragraph from Section 25

25. Certificate Renewal Verification Requirements
Before renewing an EV Certificate, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

With

25. <u>EV Certificate Renewal Verification Requirements</u>

(a) <u>Validation for Renewal Requests</u>. In conjunction with the EV Certificate Renewal process, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

(b) <u>Exceptions</u>. Notwithstanding the requirements set forth in Section 33(b) (Use of Pre-Existing Information or Documentation) and Section 8 (Maximum Validity

Period), a CA, when performing the authentication and verification tasks for EV Certificate Renewal MAY:

(1) EV Certificate previously issued by the CA:

(i) Rely on its prior authentication and verification of:

(a) A Principal Individual of a Business Entity under Section 14(b)(4) if the Principal Individual is the same as the Principal Individual verified by the CA in connection with the previously issued EV Certificate,

(b) Applicant's Place of Business under Section 16(a),

(c) The verification of telephone number of Applicant's Place of Business required by Section 16(b), but still MUST perform the verification required by Section 16(b)(2)(a),

(d) Applicant's Operational Existence under Section 17,

(e) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 19, except where a contract is in place between the CA and Applicant that specifies a specific term for the authority of the Contract Signer, and/or the Certificate Approver, and/or Certificate Requester in which case, the term specified in such contract will control,

(f) The prior verification of the email address used by the CA for independent confirmation from applicant under Section 22(d)(1)(B)(ii).

(ii) Rely on prior Verified Legal/Accountant Opinion that established:

(a) Applicant's exclusive right to use the specified domain name under Section 18 (b)(2)(A)(1) & Section 18 (b)(2)(B)(1), provided that the CA verifies that either:

a. The WHOIS record still shows the same registrant as indicated when the CA received the prior Verified Legal Opinion, or

b. The Applicant establishes domain control via a practical demonstration as detailed in Section 18(b)(2)(B)(2).

(b) Verification that Applicant is aware that it has exclusive control of the domain name, under Section 18 (a)(b)(3).

5.4 Add the following Definition to the Definition section:

EV Certificate Renewal. The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes application, to the CA that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant’s existing EV Certificate.

6. Pre-approved requests

6.1 Replace Sections 11a and 11b with the following

11. <u>EV Certificate Request Requirements</u>

(a) <u>General</u> Prior to the issuance of an EV Certificate, the CA MUST obtain from Applicant (via a Certificate Requester authorized to act on Applicant's behalf) a properly completed and signed EV Certificate Request in a form prescribed by the CA and that complies with these Guidelines. One EV Certificate Request MAY suffice for multiple EV Certificates to be issued to the same Applicant when the requests have been pre-authorized in line with section 19(d) of these Guidelines

(b) <u>Request and Certification</u> EV Certificate Requests which are not pre-authorized in line with section 19(d) of these Guidelines MUST contain a request from, or on behalf of, Applicant for the issuance of an EV certificate, or certificates, and a certification by, or on behalf of, Applicant that all of the information contained therein is true and correct.

6.2 Replace the introductory paragraph of Section 20 with the following

20. <u>Verification of Signature on Subscriber Agreement and EV Certificate Requests</u>
Both the Subscriber Agreement and each non pre-approved EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document unless the Certificate Request has been pre-authorized in line with section 19(d) of these Guidelines. If the Certificate requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases applicable signatures MUST be a legally valid and enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds Applicant to the terms of each respective document.

7. Authoritative time-source

In Appendix I, replace the paragraph that reads

"An EV Timestamp Authority MUST be synchronized with a publicly accepted time source in the jurisdiction of its operation, (e.g. NIST or Naval Laboratory in the United States)."

with

"An EV Timestamp Authority MUST be synchronized with a UTC(k) time source recognized by the International Bureau of Weights and Measures (BIPM)."

8. Phone number at place of business

Effective 4 Dec 2008, delete Section 16b and replace it with the following.

(b) Telephone Number for Applicant’s Place of Business

(1) Verification Requirements To further verify Applicant’s physical existence and business presence, as well as to assist in confirming other verification requirements, the CA MUST verify that the telephone number provided by Applicant is a main phone number for Applicant’s Place of Business.

(2) Acceptable Methods of Verification To verify Applicant’s telephone number, the CA MUST perform A and either B or C as listed below:

(A) Confirm Applicant’s telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed;

(B) Confirm that the telephone number provided by Applicant is listed as Applicant’s or Parent/Subsidiary Company’s telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or, alternatively, in either at least one Qualified Independent Information Source or Qualified Governmental Information Source, or in a Qualified Governmental Tax Information Source;

(C) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant’s telephone number, as provided, is a main phone number for Applicant’s Place of Business.

9. Minimum Cryptographic Algorithm and Key Sizes

Effective 30 Dec 2008, delete Appendix A and replace it with the following.

Appendix A

Minimum Cryptographic Algorithm and Key Sizes

1. **Root CA Certificates**

	Root Certificates whose validity period begins on or before 31 Dec 2010	Root Certificates whose validity period begins after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED),	SHA-1*, SHA-256, SHA-384 or SHA-512

	SHA-1	
RSA	2048[†]	2048
ECC	NIST P-256	NIST P-256

2. **Subordinate CA Certificates**

	Subordinate CA Certificates whose validity period begins on or before 31 Dec 2010	Subordinate CA Certificates whose validity period begins after 31 Dec 2010
Digest algorithm	SHA-1	SHA-1*, SHA-256, SHA-384 or SHA-512
RSA	1024	2048
ECC	NIST P-256	NIST P-256

3. **Subscriber Certificates**

	Subscriber Certificates whose validity period ends on or before 31 Dec 2010	Subscriber Certificates whose validity period ends after 31 Dec 2010
Digest algorithm	SHA-1	SHA1*, SHA-256, SHA-384 or SHA-512
RSA	1024	2048
ECC	NIST P-256	NIST P-256

[†] A Subscriber Certificate may, in addition, chain to an EV-enabled <2048-bit key RSA root CA certificate.

* SHA-1 SHOULD be used only until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.

10. Certificate reissuance

Effective 18 March 2009,

10.1. Replace the following section (which was itself previously amended):-

"25. EV Certificate Renewal Verification Requirements

(a) Validation for Renewal Requests. In conjunction with the EV Certificate Renewal process, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

(b) Exceptions. Notwithstanding the requirements set forth in Section 33(b) (Use of Pre-

Existing Information or Documentation) and Section 8 (Maximum Validity Period), a CA, when performing the authentication and verification tasks for EV Certificate Renewal MAY:

(1) EV Certificate previously issued by the CA:"

With:-

"25. EV Certificate Renewal Verification Requirements

(a) Validation for Renewal Requests. In conjunction with the EV Certificate Renewal process, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the renewal request is properly authorized by Applicant and that the information in the EV Certificate is still accurate and valid.

(b) Validation of Re-issuance requests. A CA may rely on previously verified information to issue a replacement certificate where:

1. The expiration date of the replacement certificate is the same as the expiration date of the currently valid EV certificate being replaced, and

2. The certificate subject of the Replacement Certificate is the same as the certificate subject contained in the currently valid EV certificate.

(c) Renewal Exceptions. Notwithstanding the requirements set forth in Section 33(b) (Use of Pre-Existing Information or Documentation) and Section 8 (Maximum Validity Period), a CA, when performing the authentication and verification tasks for EV Certificate Renewal MAY:

(1) EV Certificate previously issued by the CA:"

10.2. Replace this entry from the Definition Section (which was itself previously amended):-

"EV Certificate Renewal. The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes application, to the CA that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate."

With:-

"EV Certificate Renewal. The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes an application, to the CA that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV certificate.

EV Certificate Re-issuance. The process whereby an Applicant who has a valid unexpired and non-revoked EV certificate makes an application, to the CA that issued the original certificate, for a newly issued EV certificate for the same organizational and domain name prior to the expiration of the applicant's existing EV Certificate but with a matching ‘valid to’ date of the current EV certificate."

11. PolicyQualifierId

Effective 8 April 2009,

1. Replace the following text from Appendix B, Sections 2a and 3a:

"certificatePolicies:policyQualifiers:policyQualifierId
- id-qt 2"

with:-

"certificatePolicies:policyQualifiers:policyQualifierId
- id-qt 1"

12. Renumbering

Effective upon ratification of v1.2, renumber the Guidelines in accordance with the following table.

Proposed section number	Current section label
Front matter	Front matter, A.1.(c) Guidelines Issuing Authority, A.1.(d) Revisions to Guidelines paras 1 and 2
ToC	ToC
1. Scope	A.1.(b) Scope
2. References	Requires new material
3. Definitions	DEFINITIONS
4. Abbreviations and acronyms	Requires new material
5. Conventions	A.1.(a) para 2 General, A.1.(d) Revisions to Guidelines para 3
6. Basic concept of the EV certificate	A.1.(a) para 1 General, B. Basic concept of the EV certificate
6.1 Purpose of EV certificates	2. Purpose of EV Certificates
6.1.1 Primary Purposes	(a) Primary Purposes

6.1.2 Secondary Purposes	(b) Secondary Purposes
6.1.3 Excluded Purposes	(c) Excluded Purposes
6.2 EV certificate warranties and representations	3. EV Certificate Warranties and Representations
6.2.1 By the CA and Root CA	(a) By the CA and Root CA
6.2.2 By the Subscriber	(b) By the Subscriber
7. Community and applicability	C. COMMUNITY AND APPLICABILITY
7.1 Issuance of EV Certificates	4. Issuance of EV Certificates
7.1.1 Compliance	(a) Compliance
7.1.2 EV Policies	(b) EV Policies
7.1.3 Insurance	(c) Insurance
7.1.4 Audit Requirements	(d) Audit Requirements
7.2 Obtaining EV Certificates	5. Obtaining EV Certificates
7.2.1 General	(a) General
7.2.2 Private Organization Subjects	(b) Private Organization Subjects
7.2.3 Government Entity Subjects	(c) Government Entity Subjects
7.2.4 Business Entities	(d) Business Entities
7.2.5 Non-Commercial Entity Subjects	(d) Non-Commercial Entity Subjects
8. EV certificate content and profile	D. EV CERTIFICATE CONTENT AND PROFILE
8.1 EV Certificate Content Requirements	6. EV Certificate Content Requirements
8.1.1 Subject Organization Information	(a) Subject Organization Information
8.2 EV Certificate Policy Identification Requirements	7. EV Certificate Policy Identification Requirements
8.2.1 EV Subscriber Certificates	(a) EV Subscriber Certificates
8.2.2 EV Subordinate CA Certificates	(b) EV Subordinate CA Certificates
8.2.3 Root CA Certificates	(c) Root CA Certificates
8.3 Maximum Validity Period	8. Maximum Validity Period
8.3.1 For EV Certificate	(a) For EV Certificate
8.3.2 For Validated Data	(b) For Validated Data
8.4 Other Technical Requirements for EV Certificates	9. Other Technical Requirements for EV Certificates
9. EV Certificate request requirements	E. EV CERTIFICATE REQUEST REQUIREMENTS
9.1 General Requirements	10. General Requirements
9.1.1 Documentation Requirements	(a) Documentation Requirements

9.1.2 Role Requirements	(b) Role Requirements
9.2 EV Certificate Request Requirements	11. EV Certificate Request Requirements
9.2.1 General	(a) General
9.2.2 Request and Certification	(b) Request and Certification
9.2.3 Information Requirements	(c) Information Requirements
9.3 Subscriber Agreement Requirements	12. Subscriber Agreement Requirements
9.3.1 General	(a) General
9.3.2 Agreement Requirements	(b) Agreement Requirements
10. Information verification requirements	F. INFORMATION VERIFICATION REQUIREMENTS
10.1 General Overview	13. General Overview
10.1.1 Verification Requirements – Overview	(a) Verification Requirements – Overview
10.1.2 Acceptable Methods of Verification – Overview	(b) Acceptable Methods of Verification – Overview
10.2 Verification of Applicant's Legal Existence and Identity	14. Verification of Applicant's Legal Existence and Identity
10.2.1 Verification Requirements	(a) Verification Requirements
10.2.2 Acceptable Method of Verification	(b) Acceptable Method of Verification
10.3 Verification of Applicant's Legal Existence and Identity – Assumed Name	15. Verification of Applicant's Legal Existence and Identity – Assumed Name
10.3.1 Verification Requirements	(a) Verification Requirements
10.3.2 Acceptable Method of Verification	(b) Acceptable Method of Verification
10.4 Verification of Applicant's Physical Existence	16. Verification of Applicant's Physical Existence
10.4.1 Address of Applicant's Place of Business	(a) Address of Applicant's Place of Business
10.4.2 Telephone Number for Applicant's Place of Business	(b) Telephone Number for Applicant's Place of Business
10.5 Verification of Applicant's operational existence	17. Verification of Applicant's Operational Existence
10.5.1 Verification Requirements	(a) Verification Requirements
10.5.2 Acceptable Methods of Verification	(b) Acceptable Methods of Verification
10.6 Verification of Applicant's Domain Name	18. Verification of Applicant's Domain Name
10.6.1 Verification Requirements	(a) Verification Requirements
10.6.2 Acceptable Methods of Verification	(b) Acceptable Methods of Verification
10.7 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver	19. Verification of Name, Title and Authority of Contract Signer & Certificate

	Approver
10.7.1 Verification Requirements	(a) Verification Requirements
10.7.2 Acceptable Methods of Verification – Name, Title and Agency	(b) Acceptable Methods of Verification – Name, Title, and Agency
10.7.3 Acceptable Methods of Verification – Authorization	(c) Acceptable Methods of Verification - Authorization
10.7.4 Pre-Authorized Certificate Approver	(d) Pre-Authorized Certificate Approver
10.8 Verification of Signature on Subscriber Agreement and EV Certificate Requests	20. Verification of Signature on Subscriber Agreement and EV Certificate Requests
10.8.1 Verification Requirements	(a) Verification Requirements
10.8.2 Acceptable Methods of Signature Verification	(b) Acceptable Methods of Signature Verification
10.9 Verification of Approval of EV Certificate Request	21. Verification of Approval of EV Certificate Request
10.9.1 Verification Requirements	(a) Verification Requirements
10.9.2 Acceptable Methods of Verification	(b) Acceptable Methods of Verification
10.10 Verification of Certain Information Sources	22. Verification of Certain Information Sources
10.10.1 Verified Legal Opinion	(a) Verified Legal Opinion
10.10.2 Verified Accountant Letter	(b) Verified Accountant Letter
10.10.3 Face-to-face Validation	(c) Face-to-face validation
10.10.4 Independent confirmation from Applicant	(d) Independent Confirmation From Applicant
10.10.5 Qualified Independent Information Sources (QIIS)	(e) Qualified Independent Information Sources (QIIS)
10.10.6 Qualified Government Information Source (QGIS)	(f) Qualified Government Information Sources (QGIS)
10.10.7 Qualified Government Tax Information Source (QGTIS)	(g) Qualified Government Tax Information Sources (QGTIS)
10.11 Other Verification Requirements	23. Other Verification Requirements
10.11.1 High Risk Status	(a) High Risk Status
10.11.2 Denied Lists and Other Legal Black Lists	(b) Denied Lists and Other Legal Black Lists
10.12 Final Cross-Correlation and Due Diligence	24. Final Cross-Correlation and Due Diligence
10.13 EV Certificate Renewal Verification Requirements	25. EV Certificate Renewal Verification Requirements
10.13.1 Validation for Renewal Requests	(a) Validation for Renewal Requests
10.13.2 Validation for Reissuance Requests	(b) Validation for Reissuance Requests

10.13.3 Renewal Exceptions	(c) Renewal Exceptions
11. Certificate status checking and revocation issues	G. CERTIFICATE STATUS CHECKING AND REVOCATION ISSUES
11.1 EV Certificate Status Checking	26. EV Certificate Status Checking
11.1.1 Repository	(a) Repository
11.1.2 Reasonable User Experience	(b) Reasonable User Experience
11.1.3 Response Time	(c) Response Time
11.1.4 Deletion of Entries	(d) Deletion of Entries
11.2 EV Certificate Revocation	27. EV Certificate Revocation
11.2.1 Revocation Guidelines and Capability	(a) Revocation Guidelines and Capability
11.2.2 Revocation Events	(b) Revocation Events
11.3 EV Certificate Problem Reporting and Response Capability	28. EV Certificate Problem Reporting and Response Capability
11.3.1 Reporting	(a) Reporting
11.3.2 Investigation	(b) Investigation
11.3.3 Response	(c) Response
12. Employee and third party issues	H. EMPLOYEE AND THIRD PARTY ISSUES
12.1 Trustworthiness and Competence	29. Trustworthiness and Competence
12.1.1 Identity and Background Verification	(a) Identity and Background Verification
12.1.2 Training and Skills Level	(b) Training and Skills Level
12.1.3 Separation of Duties	(c) Separation of Duties
12.2 Delegation of Functions to Registration Authorities and Subcontractors	30. Delegation of Functions to Registration Authorities and Subcontractors
12.2.1 General	(a) General
12.2.2 Enterprise RAs	(b) Enterprise RAs
12.2.3 Guidelines Compliance Obligation	(c) Guidelines Compliance Obligation
12.2.4 Responsibility	(d) Responsibility
13. Data and record issues	I. DATA AND RECORD ISSUES
13.1 Documentation and Audit Trail Requirements	31. Documentation and Audit Trail Requirements
13.2 Document Retention	32. Document Retention
13.2.1 Audit Log Retention	(a) Audit Log Retention
13.2.2 Retention of Documentation	(b) Retention of Documentation
13.3 Reuse and Updating Information and Documentation	33. Reuse and Updating Information and Documentation

13.3.1 Use of Documentation to Support Multiple EV Certificates	(a) Use of Documentation to Support Multiple EV Certificates
13.3.2 Use of Pre-Existing Information or Documentation	(b) Use of Pre-Existing Information or Documentation
13.4 Data Security	34. Data Security
13.4.1 Objectives	(a) Objectives
13.4.2 Risk Assessment	(b) Risk Assessment
13.4.3 Security Plan	(c) Security Plan
13.4.4 Dual Access Control	(d) Dual Access Control
14. Compliance	J. COMPLIANCE
14.1 Audit Requirements	35. Audit Requirements
14.1.1 Pre-Issuance Readiness Audit	(a) Pre-Issuance Readiness Audit
14.1.2 Regular Self Audits	(b) Regular Self Audits
14.1.3 Annual Independent Audit	(c) Annual Independent Audit
14.1.4 Auditor Qualification	(d) Auditor Qualifications
14.1.5 Root Key Generation	(e) Root Key Generation
15. Other contractual compliance	K. OTHER CONTRACTUAL COMPLIANCE
15.1 Privacy/Confidentiality Issues	36. Privacy/Confidentiality Issues
15.2 Limitations on EV Certificate Liability	37. Limitations on EV Certificate Liability
15.2.1 CA Liability	(a) CA Liability
15.2.2 Root CA Indemnification	(b) Root CA Indemnification
Appendix A - Minimum Cryptographic Algorithm and Key Sizes	Appendix A — Minimum Cryptographic Algorithm and Key Sizes
Appendix B - EV Certificates Required Certificate Extensions	Appendix B — EV Certificates Required Certificate Extensions
Appendix C - User Agent Verification	Appendix C — User Agent Verification
Appendix D - Sample Form Legal Opinion Letter	Appendix D — Sample Form Legal Opinion Letter
Appendix E - Sample Accountant Letters Confirming Specified Information	Appendix E — Sample Accountant Letters Confirming Specified Information
Appendix F - Foreign Organization Name Guidelines	Appendix F — Foreign organization name guidelines
Appendix G - Code-signing: Introduction (Informative)	Appendix G — Code-Signing: Introduction
Appendix H - Code-signing: Requirements for Certification Authorities (Normative)	Appendix H — Code-Signing: Requirements for Certification Authorities
Appendix I - Code-signing: Requirements for	Appendix I — Code-Signing:

Timestamp Authorities (Normative)	Requirements for Timestamp Authorities
Appendix J - Code-signing: Requirements for Signing Authorities (Normative)	Appendix J — Code-Signing: Requirements for Signing Authorities

13. Revocation for well-known private keys

Effective 4 August 2009, delete the following paragraph from Section 27(b)3:

“The CA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the EV Certificate) has been compromised, or that the EV Certificate has otherwise been misused;”

Insert the following paragraph:

“The CA obtains reasonable evidence that the Subscriber’s Private Key (corresponding to the Public Key in the EV Certificate) has been compromised or is suspected of compromise (e.g. Debian known weak keys), or that the EV Certificate has otherwise been misused;”

14. Subject attribute requirements

Effective 5 August 2009

14.1 Delete the following paragraph from Section 6.

"6. EV Certificate Content Requirements This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of the CA and the Subject of the EV Certificate."

Insert the following paragraph:

"6. EV Certificate Content Requirements This section sets forth minimum requirements for the content of the EV Certificate as they relate to the identity of the CA and the Subject of the EV Certificate. Optional data fields within the subject DN should contain either information verified by the CA or be left empty. Meta data such as ‘.’, ‘-‘ and ‘ ‘ characters and or any other indication that the field is not applicable should not be used."

14.2 Delete the following paragraph from Section 6(a)(4).

"Contents These fields MUST contain information only at and above the level of the Incorporating Agency or Registration Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency at the country level would include country information but not state or province or locality information; the Jurisdiction of Incorporation for the applicable Incorporating Agency or

Registration Agency at the state or province level would include both country and state or province information, but not locality information; and so forth. Country information MUST be specified using the applicable ISO country code. State or province information, and locality information (where applicable), for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction."

Insert the following paragraph:

"Contents These fields MUST contain information only relevant to the level of the Incorporating Agency or Registration Agency – e.g., the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency at the country level would include country information but not state or province or locality information; the Jurisdiction of Incorporation for the applicable Incorporating Agency or Registration Agency at the state or province level would include both country and state or province information, but not locality information ; the Jurisdiction of Incorporation for the applicable Incorporating Agency or Registration Agency at locality level would include country and also state or province information where the state or province regulates the registration of the entities at the locality level. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable), for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction."

14.3 Delete the following paragraph from the Definitions Section.

"41. Jurisdiction of Incorporation: In the case of a Private Organization, the country and (where applicable) the state or province where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law."

Insert the following paragraph:

"41. Jurisdiction of Incorporation: In the case of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law."

15. Allow ETSI 102 042 audits

Effective 7 Aug 2009.

15.1 On page 3, replace:-

"Other groups that have participated in the process of developing these Guidelines include members of the Information Security Committee of the American Bar Association Section of Science & Technology Law, and WebTrust for CA. Participation by such groups does not imply their endorsement, recommendation or approval of the final product."

With:-

"Other groups that have participated in the process of developing these Guidelines include members of the Information Security Committee of the American Bar Association Section of Science & Technology Law, WebTrust for CA and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation or approval of the final product."

15.2 In Section 4.a, replace:-

"Comply with the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum; and"

With:-

"Comply with the requirements of the then-current WebTrust program for CAs v1.0 or later <http://infotech.aicpa.org/Resources/System+Security+and+Reliability/System+Reliability/Trust+Services/WebTrust+for+Certification+Authorities.htm> , completed by a licensed WebTrust for CAs auditor or ETSI TS 102 042 V2.1.1 or later <http://pda.etsi.org/pda/home.asp?wki_id=tmTZH@WhLn_.'0,.QCFnV> ; and"

15.3 In Section 4.b.1.B, replace:-

"Implement the requirements of (i) the then current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum;"

With:-

"Implement the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program or ETSI TS 102 042 V2.1.1;"

15.4 In Section 4.b, replace:-

"The CA is also REQUIRED to publicly disclose its CA business practices such as are required for public disclosure by the WebTrust for CA requirements."

With:-

"The CA is also REQUIRED to publicly disclose its CA business practices as required by WebTrust for CAs or ETSI TS 102 042 V2.1.1."

15.5 In Section 35, replace:-

"(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs (or a currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), 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, or a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.

(2) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs (or a currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), then before issuing EV Certificates the CA and its Root CA MUST successfully complete both: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, and (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, or"

With:-

"(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.

(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, and (ii) a point-in-time readiness assessment audit against the WebTrust EV Program or an ETSI TS 102 042 V2.1.1. audit, or"

15.6 In Section 35 c, replace:-

"(1) During the period in which it issues EV Certificates, the CA and its Root CA MUST undergo and pass an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such 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.

(2) Government CAs In cases where the CA is a government entity, an annual audit of the government CA by the appropriate internal government auditing agency is acceptable in lieu of the (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in the WebTrust Program for CAs and the WebTrust EV Program, and certifies that the government CA has successfully passed the audit"

With:-

"(1) During the period in which it issues EV Certificates, the CA and its Root CA MUST undergo and pass either an annual (i) WebTrust Program for CAs audit and (ii) WebTrust EV Program audit, or an ETSI TS 102 042 v2.1.1 audit. Such 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.

(2) Government CAs In cases where the CA is a government entity, an annual audit of the government CA by the appropriate internal government auditing agency is acceptable in lieu of the audits specified in (1), above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in the WebTrust Program for CAs and the WebTrust EV Program or the ETSI TS 102 042 v2.1.1. program, and certifies that the government CA has successfully passed the audit"

15.7 In Section 35 d, replace:-

"(1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and"

With:-

"(1) Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or licensed according to the laws and policies for assessors in the jurisdiction of the CA; and"

15.8 Add to the Definitions section:-

"ETSI TS 102 042 v2.1.1. European Telecommunications Standards Institute, Electronic

Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates."