Domain Names with mixed character sets with known high risk domains. If a similarity is found, then the EV Certificate Request MUST be flagged as High Risk. The CA must perform reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that the Applicant and the target in question are the same organization.

11.7 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

11.7.1 Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.

(1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agents representing the Applicant.

(2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.

(3) **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

(A) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and

(B) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and

(C) Approve EV Certificate Requests submitted by a Certificate Requester.

11.7.2 Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

(1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**

(2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:

(A) Contacting the Contract Signer and the Certificate Approver's Human Resources Department by phone or mail (at the phone number or address for the Contract Signer and the Certificate Approver, verified in accordance with these Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or

(B) Obtaining an Independent Confirmation From the Applicant (as described in Section 11.10.4), or a Verified Legal Opinion (as described in Section 11.10.1), or a Verified Accountant Letter (as described in Section 11.10.2) verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of the Applicant.

(C) Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

11.7.3 Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

(C) When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this section and is subjected to the Audit Requirements of Sections 17.5 and 17.6.

In the case of Enterprise EV Certificates to be issued in compliance with the requirements of Section 14.2 of these Guidelines, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence section.

11.13 Requirements for Re-use of Existing Documentation

11.13.1 Validation for Existing Subscribers

For each EV Certificate Request, including requests to renew existing EV Certificates, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid. However, if an Applicant has a currently valid EV Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of:

(1) The Principal Individual verified under Section 11.2.2 (4) if the individual is the same person as verified by the CA in connection with the Applicant’s previously issued and currently valid EV Certificate;

(2) The Applicant's Place of Business under Section 11.4.1;

(3) The Verified Method of Communication required by Section 11.4.2(2)(A), provided that the CA verifies the communications as required by Section 11.4.2 (2)(B);

(4) The Applicant's Operational Existence under Section 11.5;

(5) The name, title, and authority of the Contract Signer and Certificate Approver under Section 11.7; and

(6) The Applicant's right to use the specified Domain Name under Section 11.6, provided that the CA verifies that the WHOIS record still shows the same registrant as when the CA verified the specified Domain Name for the initial EV Certificate.

11.13.2 Re-issuance Requests

A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:

(1) The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and

(2) The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.

11.13.3 Age of Validated Data

(1) Except for reissuance of an EV Certificate under Section 11.13.2 and except when permitted otherwise under Section 11.13.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – thirteen months;

(B) Assumed name – thirteen months;

(C) Address of Place of Business – thirteen months;

(D) Verified Method of Communication – thirteen months;

(E) Operational Existence – – thirteen months;

(F) Domain Name – thirteen months;

(G) Identity and authority of Certificate Approver – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

(2) The dte used to determine the age of information set forth above in subsection (1) SHALL be based on CA's selection of: (a) the date that the prior EV Certificate was issued, provided that the information obtained for issuance of that EV Certificate was within thirty (30) days of that Certificate issuance; or (b) the date the information was last obtained from the appropriate source.

(3) Subject to the aging and updating requirements listed in this Section 11.13, the CA MAY use a single EV Certificate Request to issue multiple EV Certificates to an Applicant, provided that the Certificates contain the same Subjects.

(4) The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use to the extent permitted under Sections 11.8 and 11.9.

(5) The CA MUST repeat the verification processes required in these Guidelines for any information obtained earlier than the limits specified above.

12 Certificate Issuance by a Root CA

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (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.

Root CA Private Keys MUST NOT be used to sign EV Certificates.

13 Certificate Revocation and Status Checking

The requirements in Section 13 of the Baseline Requirements apply equally to EV Certificates. However, CAs MUST ensure that CRLs for an EV Certificate chain can be downloaded in no more than three (3) seconds over an analog telephone line under normal network conditions.

14 Employee and third party issues

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

(1) **Verify the Identity of Such Person:** Verification of identity MUST be performed through:

(A) The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and

(B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses);

and

(2) **Verify the Trustworthiness of Such Person:** Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:

(A) Confirmation of previous employment,