

Ballot 104 – Modification of Domain Verification under Section 11.6 of the EV Guidelines

Rich Smith of Comodo made the following motion, and Jeremy Rowley from DigiCert and Mads Henriksveen from Buypass endorsed it:

Motion Begins

EFFECTIVE IMMEDIATELY, in order to reconcile the differences in domain verification specified in the Baseline Requirements and EV Guidelines, clarify language within the EV Guidelines about the right to use a domain name, and permit additional alternatives in verifying domain control or ownership, we propose amending the EV Guidelines as follows:

4 Definitions

Capitalized Terms are defined in the Baseline Requirements except where provided below: ***

~~Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, the domain name registrar or the person or entity listed in WHOIS as the registering the domain name (including any private, anonymous, or proxy registration service) attesting that the Applicant has the exclusive right to use the specified domain name.~~

[Already defined in the Baseline Requirements, but without “exclusive right to use” language:

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.]

7 Certificate Warranties and Representations

7.1 EV Certificate Warranties

When the CA issues an EV Certificate, the CA and its Root CA represent and warrant to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Certificate is Valid, that the CA has followed the requirements of these Guidelines and its EV Policies in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate. The EV Certificate Warranties specifically include, but are not limited to, the following:

(A) Legal Existence: The CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;

(B) Identity: The CA has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject’s Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;

(C) Right to Use Domain Name: The CA has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the ~~exclusive~~ right to use all the Domain Name(s) listed in the EV Certificate. ***

11.1.1 Verification Requirements – Overview

Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, these Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following: ***

(2) Verify the Applicant is a registered holder, or has ~~exclusive~~ control, of the Domain Name(s) to be included in the EV Certificate;” ***

11.6 Verification of Applicant’s Domain Name

For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 11.1.1 of the Baseline Requirements, except that a CA MAY NOT verify a domain using the procedure described 11.1.1(7).

[BR 11.1.1(7) provides as follows – and would not be permitted for EV domain vetting:

BR 11.1.1 Authorization by Domain Name Registrant

*For each Fully-Qualified Domain Name listed in a Certificate, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either is the Domain Name Registrant or has control over the FQDN by: ****

7. Using any other method of confirmation, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant is the Domain Name Registrant or has control over the FQDN to at least the same level of assurance as those methods previously described. [Prohibited for EV domain verification.]

~~11.6.1 Verification Requirements~~

~~The CA MUST confirm that the Applicant:~~

~~(A) Is the registered holder of the Domain Name, or~~

~~(B) Has been granted the exclusive right to use the Domain Name by the registered holder of the Domain Name; To verify the Applicant's registration, or exclusive control, of the Domain Name(s) to be listed in the EV Certificate, the CA MUST verify that each such Domain Name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA). For Government Entity Applicants, the CA MAY rely on the Domain Name listed for that entity in the records of the QGIS in the Applicant's Jurisdiction.~~

~~The CA MUST compare any registration information that is publicly available from the WHOIS database with the verified Subject organization information and MUST confirm that it is neither misleading nor inconsistent.~~

~~The CA MUST further confirm that the Applicant is aware of its registration or exclusive control of the Domain Name.~~

11.6.2 Acceptable Methods of Verification

~~(1) Applicant as Registered Holder: Acceptable methods by which the CA MAY verify that the Applicant is the registered holder of the Domain Name include the following:~~

~~(A) Performing a WHOIS inquiry on the Internet for the Domain Name supplied by the Applicant, and obtaining a response indicating that the Applicant or a Parent/Subsidiary Company is the entity to which the Domain Name is registered; or~~

~~(B) Communicating with the contact listed on the WHOIS record to confirm that the Applicant is the registered holder of the Domain Name and having the contact update the WHOIS records to reflect the proper Domain Name registration. Confirmation that the registered owner of the Domain Name is a Parent/Subsidiary Company of the Applicant, or a registered trading name of the Applicant is sufficient to establish that the Applicant is the registered owner of the Domain Name;~~

~~(C) In cases where domain registration information is private, and the domain registrar offers services to forward communication to the registered domain holder, the CA MAY contact the Applicant through the domain registrar by e-mail or paper mail.~~

~~(2) Applicant's Exclusive Right to Use: In cases where the Applicant is not the registered holder of the Domain Name, the CA MUST verify the Applicant's exclusive right to use the Domain Name(s).~~

~~(A) In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, the CA MUST obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that the Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN).~~

If the Top Level Domain is a generic top level domain (gTLD) such as .com, .net, or .org in accordance with RFC 1591, the CA MUST obtain positive confirmation from the second level domain registration holder. For example, if the requested FQDN is www1.www.example.com, the CA MUST obtain positive confirmation from the domain holder of example.com.

If the Top Level Domain is a 2 letter Country Code Top Level Domain (ccTLD), the CA MUST obtain positive confirmation from the domain holder at the appropriate domain level, based on the rules of the ccTLD. For example, if the requested FQDN is www.mysite.users.internet.co.uk, the CA MUST obtain positive confirmation from the domain holder of internet.co.uk.

In addition, the CA MUST verify the Applicant's exclusive right to use the Domain Name using one of the following methods:

(i) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has the exclusive right to use the specified Domain Name in identifying itself on the Internet; or

(ii) Relying on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually agreed upon contract.

(B) In cases where the registered domain holder cannot be contacted, the CA MUST:

(i) Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant has the exclusive right to use the specified Domain Name in identifying itself on the Internet; and (ii) Rely on a representation from the Contract Signer, or the Certificate Approver, if expressly so authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the Domain Name by making an agreed upon change in information found online on a Web page identified by a uniform resource identifier containing the Applicant's FQDN.

(3) Knowledge: Acceptable methods by which the CA MAY verify that the Applicant is aware that it has exclusive control of the Domain Name include the following:

(A) Relying on a Verified Legal Opinion or a Verified Accountant Letter to the effect that the Applicant is aware that it has exclusive control of the Domain Name; or

(B) Obtaining a confirmation from the Contract Signer or Certificate Approver verifying that the Applicant is aware that it has exclusive control of the Domain Name.

(4) Mixed Character Set Domain Names: EV Certificates MAY include Domain Names containing mixed character sets only in compliance with the rules set forth by the domain registrar. The CA MUST visually compare any 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.

11.10 Verification of Certain Information Sources ***

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., ~~knowledge of its exclusive control of a Domain Name~~, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is: ***

11.10.4 Independent Confirmation From Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., ~~knowledge of its exclusive control of a Domain Name~~, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:”

(A) Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;

(B) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and

(C) Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

11.13 Requirements for Re-use of Existing Documentation ***

11.13.3 Exceptions

Notwithstanding the requirements set forth in Section ~~11.13.1~~ ~~{Error! Reference source not found. —this is in the pdf—what is the reference?}~~, when performing the authentication and verification tasks for issuing an EV Certificate where the Applicant has a current valid EV Certificate issued by the CA, a CA MAY:

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

(A) The Principal Individual of a Business Entity under Section 11.2.2 (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) The Applicant's Place of Business under Section 11.4.1;

(C) The telephone number of the Applicant's Place of Business required by Section 11.4.2, but still MUST perform the verification required by Section 11.4.2 (2)(A);

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

(E) The name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester under Section 11.7, except where a contract is in place between the CA and the 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 email address used by the CA for independent confirmation from the Applicant under Section 11.10.4 (1)(B)(ii);

(2) Rely on a prior Verified Legal Opinion or Accountant Letter that established:

(A) The Applicant's ~~exclusive~~ right to use the specified Domain Name under Section 11.6.2 (2)(A)(i) and Section 11.6.2 (2)(B)(i), provided that the CA verifies that either:

(i) The WHOIS record still shows the same registrant as indicated when the CA received the prior Verified Legal Opinion or Verified Accountant Letter, or

(ii) The Applicant establishes domain control via a process permitted under section 11.6 ~~practical demonstration as detailed in Section 11.6.2(2)(B)(ii).~~

~~(B) That the Applicant is aware that it has exclusive control of the Domain Name, under Section 11.6.1(3).~~

====Motion Ends=====

The review period for this ballot shall commence at June 25, 2013 and will close at July 2, 2013. Unless the motion is withdrawn during the review period, the voting period will start immediately thereafter and will close at July 9, 2013. Votes must be cast by posting an on-list reply to this thread.

Motion Ends

A vote in favor of the motion must indicate a clear 'yes' in the response. A vote against must indicate a clear 'no' in the response. A vote to abstain must indicate a clear 'abstain' in the response. Unclear responses will not be counted. The latest vote received from any representative of a voting member before the close of the voting period will be counted. Voting members are listed here: <http://www.cabforum.org/forum.html>

In order for the motion to be adopted, two thirds or more of the votes cast by members in the CA category and one half or more of the votes cast by members in the browser category must be in favor. Also, at least seven members must participate in the ballot, either by voting in favor, voting against, or abstaining.