Ballot 204: Forbid DTPs from doing Domain/IP Ownership Validation (Show Changes Mode)

Purpose of Ballot: At the moment, CAs are permitted to delegate the process of domain and IP address validation. However, permitting such delegations is problematic due to the way audits work - the auditing of such work may or may not be required and, if it is, those audit documents may not make it back to root programs for consideration. Although the audit situation also needs fixing, domain validation is an important enough component of a CA's core competencies that it seems wiser to remove it from the larger problem and forbid its delegation. The purpose of this ballot is to ensure that CAs or their Affiliates are always the ones performing domain/IP address ownership validation for certificates that CA is responsible for.

The following motion has been proposed by Gervase Markham of Mozilla and endorsed by Ryan Sleevi of Google and Mike Reilly of Microsoft:

-- MOTION BEGINS --
This motion modifies the Baseline Requirements.

0) In Section 1.6.1, amend definition:

> Delegated Third Party: A natural person or Legal Entity that is not the CA**, and whose activities are not within the scope of the appropriate CA audits,** but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

1) Amend Section 1.3.2 as follows:

1.3.2. Registration Authorities

With the exception of sections 3.2.2.4 and 3.2.2.5, [t]he CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

> (1) Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
> (2) Retain documentation in accordance with Section 5.5.2;
> (3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
> (4) Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.

2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the CA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 3.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

2) Amend Sec. 3.2.2.4 as follows:

3.2.2.4. Validation of Domain Authorization or Control

***

The CA SHALL confirm that, as of the date the Certificate issues, ~~*either*~~ the CA ~~*or a Delegated Third Party*~~ has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below, **or is within the Domain Namespace of a Fully-Qualified Domain Name (FQDN) that has been validated using at least one of the methods listed below (not including the method defined in section 3.2.2.4.8).** ***

3) Amend section 3.2.2.4.6 as follows:

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested FQDN by confirming one of the following under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible by the CA via HTTP/HTTPS over an Authorized Port:

1. The presence of Required Website Content contained in the content of a file or on a web page in the form of a meta tag. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or

2. The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag where the Request Token or Random Value MUST NOT appear in the request.
If a Random Value is used, the CA ~~*or Delegated Third Party*~~ SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the

Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 3.3.1 of these Guidelines or Section 11.14.3 of the EV Guidelines).

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data. If a CA wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests. This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR. E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g" The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f The CA should define in its CPS (or in a document referenced from the CPS) the format of Request Tokens it accepts.

4) In section 3.2.2.4.11 (if still present in the text at the time the ballot passes), replace the following text: "either the CA or a Delegated Third Party" with:
"the CA". [Ignoring this assuming Ballot 190 will pass.]

5) Section 8.4 is amended as follows:

8.4. TOPICS COVERED BY ASSESSMENT

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;
2. A national scheme that audits conformance to ETSI TS 102 042/ ETSI EN 319 411-1;
3. A scheme that audits conformance to ISO 21188:2006; or
4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review. Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.3.

~~*If a Delegated Third Party is not currently audited in accordance with Section 8 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 3.2.2.4 or IP address verification under 3.2.2.5 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (2) performing the domain control validation process itself.*~~

~~*If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then*~~ **For Delegated Third Parties which are not Enterprise RAs, the** CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.1, that

provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.