Drafting Team 3 Domain Name Certification - Answers to Questions

1. Who associated with the domain name registration needs to be identified and/or contacted for the purpose of Domain Name Certification?

A person who is able to demonstrate ownership or control over the domain name.

2. What is the objective achieved by identifying and/or contacting each of those entities?

By ensuring the certificate is granted only to an entity that is able to demonstrate ownership or control over the domain name, the trustworthiness of the certificate system is increased, in order to better achieve the primary goal, which is to enable efficient and secure electronic communication.

Reference: CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates version 1.5.6, (henceforth the CA/B Baseline Requirements)

section 1.4.1 Appropriate Certificate Uses

3. What might be expected of that entity with regard to the domain name?

An applicant for a Certificate must prove their control or ownership of the domain name before a certificate can be granted by a CA, which may be achieved by multiple methods, some of which use some elements of the RDS, some of which use the DNS, some of which use non-technical means, as set out in section 3,2,2.4 of the CA/B Baseline Requirements

There are three methods that use the RDS.

Method 3.2,2.4.1 is to use the RDS to confirm the applicant is the domain contact. This method may only be used if the personal identity of the domain contact has also been confirmed by methods outside the RDS (eg the methods in section 3.2.2.1 of the CA/B Baseline Requirements, or the Extended Validation equivalents, or the CA is also the registrar (see also 3.2.2..4.12)). It is to be expected that the domain contact will have consented to, and practically facilitated, the confirmation of their personal identity by means outside the RDS, if they wish to use this method, and also the CA must be able to access the domain contact data. A person identified by this means must also remain a current domain contact in order to make any certificate changes. This method requires ongoing access to domain contact personal identifying information. There may be cases where access to additional personal identifying information beyond Domain Contact name is required for disambiguation purposes, as names are not unique identifiers.

Method 3.2.2.4.2 is to use Email, Fax, SMS, or Postal Mail
This method requires the applicant to provide one of these forms of communication to the CA that is visible within the RDS and ascribed to a domain contact, accessible to the CA to use, and that the domain contact can access. It is not necessary that the applicant uses those means to reply to the CA, only that they are able to supply a Random Value communicated to them.

Method 3.2.2.4.3 is via phone.
This method requires the applicant to provide a phone number associated with the Domain Contact within the RDS, and to make that information accessible to the CA. This requires both phone information and domain contact information. This method is only effective if the information is valid and may be used to initiate a phone conversation with the domain contact.

There are multiple other methods for verifying control, that we have not described in detail, as they do not use the RDS. There are a range of technical methods that rely on demonstrating control and access to either services that are run directly under that domain name (for example, mail service 3.2.2.4.4, web sites 3.2.2.4.6, TLS 3.2.2.4.9 and 3.2.2.4.10), or the DNS itself (3.2.2..4.7).

It is worth noting that the only non-technical method of verification that does NOT also require information from the RDS, method 3.2.2.4.5, Domain Authorisation Document, will no longer be valid for use after August 2018. We recommend this method is ignored for purpose of working group deliberation at this point for that reason.

In addition to the above, we should also note the requirements for more advanced forms of certificate, the Organisational and Extended Validation Certificate, The drafting team wishes to separate discussion of these form of certificate, as this discussion is primarily to demonstrate their inapplicability for purposes of this question within this working groups scope.

Discussion of Extended Validation Certificates

1. Who associated with the domain name registration needs to be identified and/or contacted for the purpose of Domain Name Certification?

Four roles are possibly needed for an Extended Validation certificate to be issues, an authorized Certificate Requester, authorized Certificate Approver, an authorized Contract Signer, and an authorized Applicant Representative

These are natural persons who are either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant for that role (they may be a single person). These roles must be identified and validated by independent means to the RDS.
Reference. CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 11.8 and 11.9

2. What is the objective achieved by identifying and/or contacting each of those entities?

The purpose of an Extended Validation certificate is to identify the legal identity that controls a web site, and to enable Encrypted Communications.
Reference. CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 2.1 and 2.1.1
Secondary purposes include establishing business legitimacy and mitigating various forms of online identity fraud (section 2.1.2), but not establishing business honesty or trustworthiness (2.1.3)

3. What might be expected of that entity with regard to the domain name?

With regard to the applicant, it is expected that they are verified as a registered holder, or controller, of the Domain Name(s) to be included in the EV Certificate; (11.1.1. (2)).

This must be performed via one of the methods in the CA/B Baseline Requirements section 3.2.2.4. and additional checks must be performed on domain names that utilise multiple character sets.
Reference CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates version 1.6.5, section 11.7
There are additional requirements for certificates issues to .onion names, but these are not part of the Domain Name System and not relevant to this working groups scope.
There are many additional requirements for Extended Validation Certificate, but that do not vary dependent on the Domain Name, and do not utilise the RDS (and are generally required to be verified by means wholly independent of the RDS), and so are outside the scope of this working group.

So discussion of the requirements of 3.2.2.4 of the CA/B Baseline Requirements is relevant to Extended Validation Certificates, but the other requirements of Extended Validation certificates are outside the scope of this working group.