Template for defining an RDS Purpose:

Domain Name Certification

Mailing list address: gnso-rds-pdp-3@icann.org
Mailing list archive: http://mm.icann.org/pipermail/gnso-rds-pdp-3/
Coordinated by: David Cake
Members: Kal Feher, Alex Deacon, Carlton Samuels, Jeremy Malcolm, Arsen Tungali

Template for defining an RDS Purpose:
Domain Name Certification

TEMPLATE:

Purpose Name: **Domain Name Certification**

Purpose:

Information collected by a certificate authority to enable contact between the registrant, or a technical or administrative representative of the registrant, to assist in verifying that the identity of the certificate applicant is the same as the entity that controls the domain name.

Definition:

The role of a certificate authority (CA) is to bind an identity to a cryptographic key in the form of a cryptographic certificate. In the case of TLS certificate issuance the CA also needs the ability the validate and verify that the identify of the certificate applicant is the same as the entity that owns the domain name (e.g. the Registrant). While the process and rigor of CA validation and verification procedures vary, both by the nature of the certificate desired and the processes of individual CAs, the WHOIS system can be used to validate the certificate applicants ownership of control of the corresponding domain.

Tasks:

A Certificate Authority may issue certificates with different validaton levels. The three levels of validation in standard use are Domain-validated, Organisation Validation, and Extended Validation. Domain-validated certificates require only demonstration of administrative control over the domain, and so do not require interaction with the RDS, and may be validated only using the DNS (optionally including other mechanisms such as email). They are therefore of limited relevance to this purpose.

Organisation Validated certificates require identification of the organization that requests the certificate, validation methods and levels vary. We have noted Extended Validation certificates as the most explicitly relevant to the purpose, but Organisation Validated certificates are also relevant. Guidelines for the Issuance and Validation of Extended Validation certificates may be found at https://cabforum.org/wp-content/uploads/EV-V1_6_5.pdf

Extended Validation certificates explicitly identify the legal entity that controls a web site as their primary purpose. They apply only to organisations, but for Business Entitys (as defined in the EV guidelines 8.5.4) the validation process requires confirming the identity and authority of individuals applying for certificates.

At a high level Certificate Authorities may perform the following tasks.

- Confirm that the enrolling organization (requesting the certificate) is listed as the Registrant in the WHOIS

- Send one of the WHOIS contacts (registrant/admin/technical) an email to confirm domain authorization/control
- Call one of the WHOIS contacts (registrant/admin/technical) to confirm domain authorization/control

Details of how this happens are defined in the CA Browser Forum's (CABForum) Practices Section 3.2.2.4 (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.2.pdf)

Section 3.2.2.4 of the Baseline requirements is explicitly required for Extended Validation certificates by rules 11.7.1 of the Extended Validation Guidelines.

3.2.2.4. Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

The CA SHALL confirm that prior to issuance, 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 .

Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

Note: FQDNs may be listed in Subscriber Certificates using dNS Names in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permitted Subtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar. This method may only be used if:

1. The CA authenticates the Applicant's identity under BR Section 3.2.2.1 and the authority of the Applicant Representative under BR Section 3.2.5, OR

2. The CA authenticates the Applicant's identity under EV Guidelines Section 11.2 and the agency of the Certificate Approver under EV Guidelines Section 11.8; OR

3. The CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Template for defining an RDS Purpose:
Domain Name Certification

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

The CA or Delegated Third Party MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA or Delegated Third Party MAY resend the email, fax, SMS, or postal mail in its entirety, including re- use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. The CA or Delegated Third Party MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at- sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email MAY confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed

Template for defining an RDS Purpose:
Domain Name Certification

The Random Value SHALL be unique in each email.

The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient SHALL remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

Note:

This group did not find that access to all RDS data was required in all cases, but was required for some CA validation methods.

Users: Describe the parties who often access gTLD registration data in pursuit of this purpose.

Employees of Certificate Authorities and automated systems associated with Certificate Authorities responsible for preforming the validation and verification as described above.

Data: List of gTLD registration data often involved in this purpose – for contact data, please identify the data subject (e.g., registrant, tech contact, registrar, etc.) and data element(s) as applicable.

Data Element	**Purpose**
Domain Name	To match with FQDN placed into the certificate.
Registrant, Tech and Admin *Email*	A means to contact the owner of the domain name, using manual or automated processes, with the goal of confirming that the identity of the certificate applicant is the same as entity that owns the domain name.
Registrant, Tech and Admin *Phone*	Used as an alternative method of contact in curcumstances where Email is not available or when an additional level of manual or automated verification is needed.
Registrant, Tech and Admin *Name*	Used when necessary to confirm an individual can or does work for or represent the applying organization.
Registrant, Tech and Admin Postal *Address (Street, City, State/Province, Country)*	Used to confirm that the organization of the entity that owns the domain name matches the organization of the of the certificate applicant. Also used in authentication/verification scenarios that are postal mail based.

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.

Working Group Notes 10 March 2018, ICANN61 F2F

Domain Name Certification

- DT3 Answers: DT3AnswerstoQuestions-8March.pdf

WG Response:

- Who is the certifying agent? The CA itself
- This purpose is only relevant to those registrants that want a certificate; access could be provided by some kind of one-time-use token and not publication of data
- When DN is sold, is the certificate revoked?
- ICP in China and SSL: having public email makes it much easier. We face difficulties with .co.uk to get SSL validation, because email is not available in WHOIS by design
- In cases where email address is published in WHOIS, obtaining a certificate may be easier, but email-based validation is not the only method available and not having an email address doesn't prevent obtaining a certificate
- If a CA (other than the CA run by the registrar) wants access to data to provide their service they could pay the registrar to get access. These kinds of business model issues are out of scope of this PDP.