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**

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 website 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.

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

The Random Value SHALL be unique in each email.

Template for defining an RDS Purpose:
Domain Name Certification

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.

For easy reference, below is an excerpt from the EWG Final Report:

Domain Name Certification	Tasks within the scope of this purpose include a Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name. To accomplish this task, the user needs to confirm that the DN is registered to the certificate subject; doing so requires access to all public and gated data about the Registrant.

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.

Registry/Registrant "IDs"

Registrant, Tech Contact and Admin Contact

- Name
- Organization
- Street
- City
- State/Province
- Postal Code
- Country
- Phone
- Phone Ext
- Fax
- Fax Ext
- Email

Template for defining an RDS Purpose:
Domain Name Certification