Certification Services Use Case

Goal: Certification Authorities (CAs) receive requests to generate and sign digital certificates on behalf of domain name operators. Several CAs offer certificate products at price points tied to the amount of registrant information validation performed by the CA. At the low end of the scale the CA performs minimal data validation. At the high end of the scale the CA validates much more data, often using manual processes. The goal of this use case is to describe the role of the gTLD Directory Service in this process.

Use Case Summary: Help a certification authority to determine and validate the identity of the entity associated with a domain name that will be bound to an SSL/TLS certificate.

Use Case Description: An Applicant contacts a person or automated process associated with a CA with a request to create a digital certificate that is bound to a domain name. The CA asks the applicant to provide the domain name in the form of a Certificate Signing Request (CSR). The CA retrieves and decodes the CSR and accesses an online resource for displaying contact information associated with registered domain names under a TLD or TLDs. The CA submits the domain name to the online resource for processing. The resource returns information associated with the domain name that includes entities that can be contacted and entity metadata that can be validated to confirm the identity of the Applicant. The CA then uses the retrieved information (sends email to the registrant or technical contact email address and waits for a reply, compares address information to public records, etc.) to confirm that the Applicant has the exclusive right to use the specified domain name. The certificate generation process typically fails if the information provided by the Applicant cannot be matched to information published in the Directory Service.

Primary Actor: CA that is attempting to validate Applicant-provided information.

Other stakeholders: Registered domain name registrant or entity operating on behalf of the registrant, operator of the gTLD Directory Service for the queried domain name, registered domain name registrar or hosting provider (who may be providing an operational service to generate a CSR or provide a proxy service), proxy service provider, Certification Authority.

Data Elements: Data elements that uniquely identify the certificate Applicant are the most useful in the context of this use case, and most CAs routinely use the data from WHOIS records as the starting point for uniquely identifying the certificate Applicant.. At the low end of the certificate service scale (for DV/domain-validated certificates) these include items that can be validated in near-real time through direct contact, such as an email address, an instant messaging address, and a telephone number. At the mid and higher end of the certificate service scale (for OV/organization-validated certificates or EV/extended validation certificates) this would include personal names, an organization name, and a postal address [Sanjay and Cecilia, please advise on other fields/data elements that are used].

Certification Services Use Case

> **Consequences of inability to access WHOIS data**: without access to WHOIS data, CAs will not be compliant with the CA/Broswer Forum's requirement to use WHOIS (https://cabforum.org/2010/03/26/ballot-36-public-whois-information/), and the time required to validate identities will be increased, and it is likely that the costs of certificates will increase.