Privacy/Proxy Service Provider Applicant Guide

ICANN Privacy and Proxy Service Provider Accreditation Program
[IRT Discussion Draft v1] | May 2017

Contents

Executive Summary

The ICANN organization is implementing a Privacy and Proxy Service Provider Accreditation Program pursuant to Final Policy Recommendations developed by the community Policy Development Process. These Recommendations were approved by the ICANN Board of Directors in August, 2016.

Privacy and Proxy Services provide a mechanism for entities to register and utilize domain names without listing personal contact information in the public Registration Data Directory Service (RDDS).
-Proxy Services mask a customer's name and contact information in the RDDS. The Proxy Service becomes the Registered Name Holder (Registrant) and licenses use of the name to the customer.
-Privacy Services generally mask all of a customer's contact information in the RDDS other than the customer's name. As a result, the customer of a Privacy Service remains the Registered Name Holder (Registrant).

Any entity that provides these services is considered a Privacy and/or Proxy Service Provider.

Prior to the launch of this Accreditation Program, the 2013 Registrar Accreditation Agreement included a limited set of requirements for Privacy and Proxy Service Providers that registrars are required to follow and pass down to their Affiliates and Resellers.[1] Once this new Accreditation Program is fully implemented, the interim requirements in the RAA will be replaced with the new Accreditation Program requirements. ICANN-accredited registrars will be prohibited from knowingly accepting registrations from Privacy and Proxy Service Providers that are not accredited by ICANN.[2] This Program creates uniform requirements for Privacy and Proxy Service Providers related to (a) the relay of communications to customers from third parties; (b) abuse reporting; (c) Provider terms and conditions; (d) Registration Data Directory Service labeling; and (e) responses to requests from public safety authorities and intellectual property holders.

This accreditation program is modeled after the ICANN organization's gTLD Registrar Accreditation Program. Privacy and Proxy Services are frequently offered by registrars and their Affiliates.[3]

---

[1] See 2013 RAA, Specification on Privacy and Proxy Registrations, https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#privacy-proxy.

[2] See Final Report, http://gnso.icann.org/en/issues/raa/ppsai-final-07dec15-en.pdf, at p. 7.

[3] The Registrar Accreditation Agreement, at Section 1.3, defines "Affiliate" as "a person or entity that, directly or indirectly, through one or more intermediaries, Controls, is controlled by, or is under common control with, the person or entity specified."

This guidebook explains the processes and criteria for Provider accreditation. The accreditation program will be launched in two phases: (1) the initial application phase, followed by (2) the program maintenance phase.

On the implementation effective date (to be determined at the conclusion of the Implementation Review Team's work), the ICANN organization will begin accepting applications from entities that are interested in becoming accredited Privacy and Proxy Service Providers during the initial application phase. At the close of this phase, ICANN will announce a list of newly accredited Providers. Following this announcement, the Program will transition to the program maintenance period, when applications for accreditation will be received and evaluated on an ongoing basis.

For additional information, please consult the ICANN website: [add URL here]

<div style="border:1px solid #8ab;padding:4px;">
Commented [AB1]: Note to IRT: Ultimately, this will include a link to an area of the ICANN website with information about the program (page not yet created).
</div>

Initial Application Window

During the initial application window, Privacy and Proxy Service Providers will be permitted to apply for accreditation during a time-limited application submission period.

The ICANN organization will announce the list of newly accredited Privacy and Proxy Service Providers after all applications submitted during the initial application window have been evaluated by (a) posting a list of the providers on ICANN.org and (b) notifying all ICANN-accredited registrars of the newly accredited providers. If a particular application cannot be processed during the preliminary application window due to incomplete or incorrect answers, or due to an applicant's failure to adequately respond to one round of follow-up questions within the required time period, the applicant may elect to re-apply during--or defer the processing of its application to--the program maintenance phase.

A proposed schedule for the initial application window is as follows:[4]

Month 1:   Final Accreditation Program requirements, including Policy, Accreditation Agreement, application for accreditation and effective date announced.

Month 3:   Initial application window opens. Providers may apply for accreditation during 90-day window. As successful completion of educational program is required to

---

[4] Processing times will become available as criteria are more thoroughly defined.

proceed to accreditation during this phase, applicants are encouraged to apply as early as possible.

Month 6:   Deadline for applications to be submitted during early application window. The ICANN organization continues evaluation of applications received during initial application window.

Month 9:   Application processing status update to be shared with community.

Month 12:   Target date for ICANN to announce list of first group of accredited providers. Actual date could be earlier or later, depending on processing time.

Program Maintenance Phase

Following ICANN's announcement of the list of the first group of accredited providers and the close of the initial application window, the Accreditation Program will transition to the program maintenance phase.

The program maintenance phase will entail ongoing program management, including:
- Continual receipt and processing of applications for accreditation;
- Privacy/Proxy Service Provider account management;
- Ongoing outreach, engagement and education; and
- Launch of the Privacy and Proxy Service Provider Compliance Program.

Accreditation Criteria

In order to obtain ICANN accreditation to provide Privacy and/or Proxy Services, an entity must demonstrate:

- Understanding of and ability to comply with Policy and Contractual requirements, as demonstrated through answers to application questions and successful completion of provider educational program.
- Evidence of sufficient capital available for the operation of the Privacy and/or Proxy Service.
- Tier III data center certification or evidence that facilities are Tier III equivalent.
- Robust and scalable operations capable of handling the customer volume reasonably projected by the applicant.
- A reliable and readily usable data backup and archival solution for all required customer data.
- The capacity to engage a sufficient number of qualified employees to handle the applicant's business operations.
- Planning for the occurrence of security breaches, natural disasters, infrastructure and/or business failure.

ICANN may conduct a background screening on applicants and individuals named in the application.

During the background screening process, ICANN may examine whether any entity or individual named in the application has a conviction or decision of the types listed in (a)-(j) below:

(a) is convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged by a court of competent jurisdiction to have:

(b) committed fraud,

(c) committed a breach of fiduciary duty, or

(d) with actual knowledge (or through gross negligence) permitted illegal activity in the registration or use of domain names or in the provision to registrar by any Registered Name Holder of inaccurate WHOIS information; or

(e) failed to comply with the terms of an order issued by a court of competent jurisdiction relating to the use of domain names sponsored by the registrar and/or protected by the applicant's Privacy and/or Proxy Service;

(f) or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing; or

(g) is disciplined by the government of its domicile for conduct involving dishonesty or misuse of funds of others; or

(h) is the subject of a non-interlocutory order issued by a court or arbitral tribunal, in each case of competent jurisdiction, finding that the applicant has, directly or through an Affiliate, committed a specific violation(s) of applicable national law or governmental regulation relating to cybersquatting or its equivalent; or

(i) is found by ICANN, based on its review of the findings of arbitral tribunals, to have been engaged, either directly or through its Affiliate, in a pattern and practice of trafficking in or use of domain names identical or confusingly similar to a trademark or service mark of a third party in which the Registered Name Holder has no rights or legitimate interest, which trademarks have been registered and are being used in bad faith.

(j) applicant knowingly employs any officer that is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such officer is not terminated within thirty (30) days of Applicant's knowledge of the foregoing; or any member of Applicant's board of directors or similar governing body is convicted of a misdemeanor related to financial activities or of any felony, or is judged by a court of competent jurisdiction to have committed fraud or breach of fiduciary duty, or is the subject of a judicial determination that ICANN reasonably deems as the substantive equivalent of any of the foregoing and such member is not removed from Applicant's board of directors or similar governing body within thirty (30) days of Applicant's knowledge of the foregoing.

Application for Accreditation

A. General Information
1. Legal Name of Privacy/Proxy Service Provider (hereinafter, "Provider"), including any fictitious/"DBA" names used:
2. Designated primary contact person for Provider:
3. Business Address:
4. Jurisdiction and type of entity (e.g. California non-profit corporation):
5. Telephone number:
6. Email address:

B. Registrar Relationship
1. Is the Provider Affiliated (as the term is defined in the Privacy and Proxy Service Provider Accreditation Agreement)[5] with an ICANN-accredited registrar(s)? (If yes, please list the registrar(s) and the registrar IANA ID(s) and provide a description and/or diagram of the corporate structure).

C. Background Screening (note that background checks may be conducted on any or all entities and individuals identified in this section)
(a) Provide the full names of all owners/shareholders of the applicant entity that own at least 5% of the company, as well as all directors, officers, and managers who will be involved in providing privacy/proxy services:

(b) Within the last ten (10) years, has the applicant or any of the people or entities listed above been charged with or convicted of a felony or of a misdemeanor related to financial activities, fraud, breach of fiduciary duty or dishonesty, or been the subject of a judicial or administrative determination that is similar or related to any of these? If so, identify them:

(c) Within the last ten (10) years, has the applicant or any of the people or entities listed above been investigated or disciplined by the government of its, her, or his domicile for conduct involving dishonesty or misuse of funds of others? Is so, identify them:

(d) Is the applicant or any of the people or entities listed above currently involved in any judicial, administrative, or regulatory proceeding that could result in a conviction, judgment, determination, or discipline of the type specified in "b" or "c" above? If so, identify them:

---

[5] Section to be cited after draft agreement is finalized for public comment.

(e) Has the applicant or any of the people or entities listed above been declined by ICANN of registrar accreditation?

D.   Business Operations
1. Does the applicant currently offer privacy and/or proxy registration services? If so, which one(s)?
2. If so, how long has the applicant offered these services?
3. How many customers does your privacy/proxy service currently service?
4. What volume of registrations do you anticipate servicing under this accreditation?
5. How will your privacy/proxy service notify existing customers of any new requirements, processes and/or contractual provisions related to obtaining this accreditation?
6. Provide a description of the services the applicant intends to offer using this privacy/proxy service accreditation. (e.g. Is the applicant going to offer privacy services, proxy services, or both? Does the applicant provide other services, such as registrar, reseller, hosting, etc?)
7. How will the privacy/proxy customer use the privacy/proxy service during the domain registration process? (e.g. will this be provided as an option through the registrar interface, will the service register names on behalf of its customers, etc?)
8. How many employees are associated with the applicant, and how many will be involved in the operation and support of privacy/proxy services? Note how many full-time employees will be responsible for customer service, including responding to third-party requests.

E.   Policy Requirements
1. Identify the steps (in detail) the Provider will take to validate and verify your customers' contact information.
2. Describe how the Provider will comply with the ICANN Transfer Policy when the privacy/proxy service is activated and/or terminated for a customer.
3. Describe the steps the Provider will take to avoid the need to disclose underlying customer data in the process of renewing, transferring or restoring a domain name.
4. Describe the steps the Provider will take to ensure continued operations for its customers (and privacy for customer data) in the event the Provider goes out of business or becomes de-accredited for some other reason.
5. Describe the steps the Provider will take to ensure the security of its customers' information, including identifying and account information and other data, including payment information.
6. How will your Provider ensure that domain name registrations utilizing your service are clearly labeled as such in the Registration Data Directory Service?

F.   Recordkeeping
1. How will the Provider ensure that customer data is escrowed in compliance with its Accreditation Agreement requirements?

2. Describe the Provider's processes for maintaining records on the number and type of relay, disclosure and publication requests received, and the number honored.

G. **Third-Party Requests**
1. Describe the process and criteria the Provider will use to determine whether or not to relay communications from a third party to the privacy/proxy customer.
2. Describe the process and criteria the Provider will use to determine whether or to disclose or publish a customer's identity or contact details in response to a third-party request (Do not include specific processes for intellectual property or law enforcement-related requests here, additional questions follow).
3. Provide a link to the webpage where third parties can initiate a request for relay, disclosure or publication of your customers' contact information. Note, this location should also include a mechanism for a third party to escalate or follow up on a request.
4. Describe the processes the Provider will follow when it receives a request for disclosure from an intellectual property holder.
5. Describe the processes the Provider will follow when it receives a request for disclosure from law enforcement.

H. **Abuse Reporting**
1. Describe, in detail, the Provider's process for managing claims of abuse.

I. **Customer Agreement/Terms of Service**
1. Identify where, in your customer agreement/terms of service (submitted with this application) the following terms appear:

    (a) any specific requirements applying to transfers and renewals of a domain name;

    (b) pricing;

    (c) the specific grounds under which a customer's details may be disclosed or published;

    (d) the specific grounds under which a customer's privacy/proxy service may be suspended or terminated, including publication in the event of a customer's initiation of a transfer of the underlying domain name;

    (e) clarification as to whether or not a customer will be notified when the privacy/proxy service provider receives a request for disclosure or publication and whether the customer may opt to cancel the domain registration in lieu of disclosure or publication;

2. Provide a link to the page where your privacy/proxy service terms of service are displayed on your website.
3. Provide a link to the page where privacy/proxy service contact information is displayed on your website.

J. **Required Appendices**
Business registration certificate
Verified financial statement

One World, One Internet