SSAC Position re:

Protecting Legal vs Natural Persons

Steve Crocker

14 April 2021: This is a partial draft. Several parts remain to be written.

## The role of roles in the registration system

Before discussing the rules governing disclosure of registration data related to natural versus legal persons, we begin with some observations about the registration process. This section covers the various roles.

### 1.1 The Account Holder and the Registrant

The privacy issues related to the various roles and status of the registration start with the registration process. While the following may seem both basic and unrelated to the privacy issues, there are a couple of essential points that come into play.

Registration of a domain name is done by an Account Holder (AH). This is the person who has the account with the registrar. In many contexts, particularly when viewed from registrar’s perspective, the Account Holder is referred to as the Customer.

The AH interacts with the Registrar to choose a domain name, provide the info related to the Registrant and possibly other roles, make payment, and populate the DNS records. The AH has an account with the Registrar. The AH has the electronic keys to the domain and can make changes at will.

The Registrant, sometimes called the Registered Name Holder (RNH), has official authority over the domain registration. As soon as the AH fills in the name of the Registrant, the Registrant acquires official, legal control over the domain registration. Occasionally there are conflicts or miscommunication between the AH and the Registrant. These conflicts are usually resolved in favor of the Registrant if the Registrant has the necessary documentation. Resolution usually requires days to weeks. In contrast, the AH has immediate access to the registration and can make changes within seconds or minutes.

With respect to informed consent, the AH necessarily is informed about the details of the registration. In principle the Registrant is also informed and has consented to be the Registrant, but sometimes this does not happen. Nonetheless, this is an essential requirement and a prerequisite for all that follows.

We note the role of the Account Holder is usually not mentioned in discussions about registration data. The Account Holder is usually known only to the registrar and is generally not shared with the registry. Nonetheless, the role of the Account Holder is fundamental and cannot be left out of any discussion related to the registration process.

### 1.2 The Admin, Tech and other Contacts

In the course of registration, the AH may also provide contact data for other roles. The most common other roles are the Admin and Tech contacts, but Billing and other roles are sometimes used. The Admin and Tech Contacts arose in the earliest days of the Arpanet, before the Internet and before the domain name system. They were the administrators of the time-shared computers that were the hosts on the Arpanet. These roles were created, and the names published, to make it possible for these people to reach other when there were operational problems on the Arpanet. That era was several decades ago when the total number of users was numbered in the thousands, not billions. **In the modern era, these roles have no standard definition or use.** Some registrars assign a limited role to the Admin Contact to authorize transfers, but this is not standardized across the Internet domain name registration system. These roles are, for the most part, anachronisms that have no defined and stable meaning. As a consequence, the data for these roles are often blank, meaningless, or simply a copy of the registrant’s data.

### 1.3 The Fundamental Rule of Roles

From a system design point of view, in order for a role to be a meaningful part of the system, two attributes must be defined, authority and responsibility. Authority is the set of actions the person in the role is authorized to, i.e. may, take. Responsibility is the set of actions the person in the role is obligated to, i.e. must, take. Further, the authority and responsibility must be understood by both the person named and by everyone who contacts the person in that role.

This may seem like common sense, and indeed I hope it does seem so. Strangely, though, there are plenty of cases where a person does not even know they’ve been named in a role. This is a gap in the design of the DNS registration system that needs to be remedied. The rules governing the registration system must be amended to include the following three requirements.

* For each role included in a registrar’s registration system, there must be a definition of the authority and responsibility associated with that role.
* The definition(s) must be available to everyone, i.e. both the people named in the roles and others who may contact the people in those roles.
* The people named in the roles must be informed that they have been named and must agree to accept the responsibility and to exercise the authority.

This last point, in addition to remedying an important existing weakness in the registration system, provides the basis for establishing the rules and procedures for protecting the privacy of the individuals named in these roles.

We make this point not as a recommendation in the context of conveying an SSAC position with respect to developing an ICANN policy on privacy. Rather, we make this point as an identification of an existing flaw in the design of the system that must be remedied. This is not a recommendation; it is a requirement.

### 1.4 But What About Existing Registrations?

There are more than one hundred million registrations that exist within the ICANN contractual system. Almost all of them contain fields that hold the data elements for an Admin Contact and Tech Contact. What is the intended remedy for these existing registrations? A simple declaration will do the job. Each registrar should publish a statement spelling out the authority and responsibility assigned to each role. If there is no authority or responsibility, the declaration only needs to say so. For example:

The Admin and Tech Contacts are carried over from the earliest days of the network. At the present time, there are no specific authority or responsibility associated with these roles.

Further, the notice from the registrar to the registrant must require the registrant inform any named contacts. In what follows, we take as a given the people named in the various roles have indeed been informed of their authority and responsibility and have agreed to adhere to these.

In the future, these roles should either be phased out or defined. Further, unless the defined roles are essential to the operation of the overall registration system, they should be optional.

## The Registration Process

During the course of registration of a domain name, all five of the following take place.

* A domain name is reserved
* Payment is made
* The status of the registrant is determined
* The registrar collects data related to the domain name and data related to the registrant.
* Levels of protection are assigned to each of the collected data elements.

In addition, the registrar may test the accuracy of some of the data elements. This is an important part of the registration process but mostly outside the scope of the present discussion. (However, see TK for a recommendation related to the accuracy of the data.)

The term “status” here refers roughly to whether the registrant is a legal or natural person, but it also includes a bit more. The status is used to determine whether certain data is required, optional or not collected, and also to determine what level of sensitivity to assign to each data element. The term “sensitivity” is part of the framework that determines which data elements are to be made available to which requesters. Some but not all of the data elements will be available to any requester without restriction. In shorthand these data elements are thus “public,” but it’s helpful to use more precise terminology. See TK for details.

The most common effect of classifying some registrants as natural persons and some as legal persons is to mark certain data elements associated with a natural person as restricted and to mark the same data elements associated with a legal person as public. However, other factors may override this effect. A natural person may wish to have some of their data elements made available to any requester. Conversely, a legal person may have reasons to keep some of their data elements unavailable to general requests.

Determination of the status, i.e. whether the registrant is a natural or legal person and whether there are other relevant factors, is thus not a limited and automatic process. As a consequence, the registration process may involve multiple steps.

### 2.2 The Order of Events

It’s helpful to view the registration process in three steps as depicted in Figure 1:

1. Preliminary interaction to gather information.
2. Classification of the registrant as a natural person or a legal person and acquisition of any other relevant factors.
3. Completion of the registration by acquisition of any additional required data.

The purpose in presenting the process in this fashion is to call specific attention to the determination of the registrant’s status and to leave room for the remainder of the registration process to depend on this determination. Further, there will be variation among the registrars. One class of approaches are explicit determination of the registrant’s status. Examples of explicit determination include the following.



1. **Separate paths:** The registrar requires the Account Holder to state whether the registration is for a natural vs a legal person and whether the registrant requires special protection. The remainder of the registration process is determined by the answers.
2. **Businesses only:** The registrar serves only businesses. The “preliminary interaction” need only be a declaration the registrant is expected to be a legal person and will be treated as such.
3. **Real people only:** The registrar serves only natural persons. Every registrant must be a natural person, with a registrar’s declaration similar to the previous approach.
4. **Common form with explicit questions:** The registrar’s form includes an explicit question as to the registrant’s status.

Figure : General Registration Flow

In each of these approaches, the Account Holder explicitly provides the necessary data to determine the status. If incorrect data is provided by the Account Holder, the burden is on the registrant.

In contrast, there are approaches where the registrar infers the status of the registrant based on less explicit information. One common approach is to infer the registrant is a legal person if the Org field is filled in. This is problematic because the registrar is making the determination. If the registrar’s decision is incorrect, the registrar may bear some risk.

### 2.3 Unknown status

What happens if the registrar is unable to determine the status of the registrant? There are two broad reasons this might happen. Determining the status of the registrant has not previously been a requirement, so the bulks of the very large number of existing registrations are currently of unknown status. The uncertainty can also arise for new registrations if the account holder does not provide details during the registration process. The registrar is then faced with either refusing to complete the registration or accept it with incomplete knowledge of the status.

Rather than attempting to establish the precise status of all existing and new registrations, it is useful and practical to include a third classification of “unknown” for both the person and whether the person requires special protection. This approach leads to nine possible classification of status, either natural person, legal person, or unknown paired with either normal registrant, protected registrant or unknown protection status. Recalling the reasons for collecting this data about the registrant’s status is to determine which data elements must be collected or are optional and what level of protection is to be applied to each of the collected data elements. In principle, a registrar might have as many as nine distinct sets of rules corresponding to each of the nine combinations. In practice, the registrant is likely to groups many of these cases together. One likely approach is to treat unknown status of natural vs legal the same as natural. Similarly, many registrars will treat uncertainty as to whether special protection is required as to assume special protection is not required. Alternatively, some registrars may not offer special protection.

## Accommodating Variation and Change

### 3.1 Variation across Registrars

Not all registrars operate the same way. It’s important to identify which aspects of a policy must be the same across all of the contracted parties and which aspects may vary according to the business needs or practices of the registrar.

The most common variation is whether specific data elements are required, optional or not collected. As a small but relevant example, not all registrants have fax numbers. Some registrars provide a field for a fax number, but others do not. An example of a possible ICANN policy is to permit a registrar to do either of these, but not to allow a registrar to require a fax number.

More generally, the ICANN policy should indicate which details must be the same in all registrars and which details are at the discretion of the individual registrar.

### 3.2 Change over Time

One area of current discussion is whether the registrant must be allowed to specify that some or all of their data is to be made available to anyone. Many registrars do not yet provide the capability for allowing the registrant to make this choice. However, it is anticipated that all registrars must provide this capability in the future. This is an example of a change that will occur in the future. Part of the policy discussion and decision process should include a way of specifying multiple policies and identifying which of these are current policy, definite future policy or proposals that are not yet adopted.

## Requests

[This section is in progress]

Requester

Registrar

Request

Accept?

Select Data Elements

Refusal

Response

## Summary of Requirements and Recommendations

1. **Inescapable Requirement: Definition of Roles**
Each role must be defined in terms of the authority and responsibilities associated with the role. This definition must be explicitly available to both the people fulfilling the role and the people interacting with the people in those roles. Each person named in a role must be aware of being named and must agree to the obligations associated with the role.

The definition must also include an explicit statement of how the information about the person in the role will be disseminated.

Information about the registrant is provided by the Account Holder. The Account Holder is effectively an agent of the Registrant and is the only authoritative source of information about the status of the registrant.
2. **Recommendation: Unknown Persons**
In addition to definite status of Natural Person or Legal Person, the status of Unknown should be included in the design of the system.
3. **Recommendation: Additional Protection**
In addition to whether the registrant is a Natural, Legal or Unknown Person, the status should also include an additional attribute regarding whether the registrant requires special privacy protection.

It is an open question as to whether additional privacy protection should be available to any registrant who wishes it or should require justification. At the very least, to facilitate visibility into potentially harmful behaviors, Registrars should avoid unnecessary protection of registration data.
4. **Recommendation: Downgrading**
Registrants should have the option of “downgrading” the level of protection for some or all of their data elements.

Registrars should have the option of implementing downgrading on a field by field basis or in groups of fields.

ICANN should establish a date certain for registrars to implement registrant option to downgrade the sensitivity of their registrations.
5. **Comment: Recourse**
 If a person named in any role in a registration feels the data is incorrect or is being disseminated improperly, they have recourse via the Registrant. Failing that, they have recourse through ICANN’s compliance process. No additional processes are required.
6. **Recommendation: Org Field**
The Org field should not be used to determine the registrant’s status. The Registrar should require Legal Persons to provide the Org data element. The Registrar should permit Natural or Unknown registrants to provide or not provide the Org data element.
7. **Recommendation: Transition**
ICANN should establish a plan for transitioning Unknown registrations into known status.