# Consideration of Multiple Changes and the Inclusion of DNS OperationsInput to the Transfer Policy Review (TPR) Working Group

Steve Crocker, invited subject matter expert

15 May 2021

## Transfer Scenarios

The charter distinguishes between inter-registrant and inter-registrar transfers. A natural question is whether it is possible to change both the registrant and registrar change at the same time.

A separate issue is the disposition of the registrant’s DNS service. For some transfers, e.g. the sale of a parked domain that is not in active use, there’s no need to worry about the DNS service. However, in situations when the domain is in active use, it may be important for the DNS service to continue without interruption.

During the call on Friday, I suggested a two-by-two matrix of possibilities: Registrar transfer or Registrant transfer as one dimension and transfer or no transfer of the DNS service as the other dimension. After some more thought, I realized the list of possibilities is a bit longer. The registration transfer might be:

* No transfer (included for completeness)
* Change of Registrant (New Rt)
* Change of Registrar (New Rr)
* Change of both Registrant and Registrar (New Rt; New Rr)

At the same time, there are three possibilities pertaining to the DNS service:

* No change
* Transfer of unsigned DNS service (Unsigned xfr)
* Transfer of DNSSEC signed service (Signed xfr)

These two effects create a total of twelve possible scenarios, including the null scenario where nothing changes. The following table presents these in tabular form, with the null scenario numbered 0.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenario | New Rt | New Rr | DNS | DNSSEC |
| 0 | No change |  |  |  |  |
| 1 | Unsigned xfr |  |  | √ |  |
| 2 | Signed xfr |  |  | √ | √ |
| 3 | New Rr |  | √ |  |  |
| 4 | New Rr; unsigned xfr |  | √ | √ |  |
| 5 | New Rr; signed xfr |  | √ | √ | √ |
| 6 | New Rt | √ |  |  |  |
| 7 | New Rt; unsigned xfr | √ |  | √ |  |
| 8 | New Rt; signed xfr | √ |  | √ | √ |
| 9 | New Rt; new Rr | √ | √ |  |  |
| 10 | New Rt; new Rr; unsigned xfr | √ | √ | √ |  |
| 11 | New Rt; new Rr; signed xfr | √ | √ | √ | √ |

## One at a time or all at once?

Is it necessary to consider all the scenarios? Should we focus on the scenarios involving just a single change, e.g. scenarios 3 and 6, or should we focus on scenario 11, the most difficult scenario.

In my experience, both approaches are important. It is much easier to think through the details of a single change. This is a good starting point in the design process. It helps build intuition and understanding of the necessary steps.

However, thinking through the details of each of the single change scenarios is not enough. There are usually complications involved in making multiple changes at the same time. Some may view these as “corner cases,” which carries the connotation these are rare and possibly unimportant. I prefer to refer to this as the most general case. If it’s possible to handle the general case, then each of the other scenarios will also be covered. Many of the other scenarios will be simpler, of course. However, I would not recommend focusing only the simple scenarios. This is the time to cover the full range of possibilities.

Thus, in response to the questions I posed in the first paragraph of this section, we should focus on both the scenarios involving a single change and the scenario where everything changes at the same time.

## A few words about transferring DNS service

Changing DNS providers while maintaining continuity of service has some technical challenges. The main requirement is to bring up service under the new operator and have it in operation in parallel with the existing service. To do this, the name servers of the new operator must be added to the list of name servers for the domain in the old operation. This requires technical and administrative cooperation from the losing operator.

If the zone is signed separately by each operator, there is an added requirement of including the key(s) of each operator in the keysets of each operator. Again, this requires specific cooperation from the losing operator. Worse, yet, neither existing DNSSEC protocol standards nor the software packages from the major DNS software providers, e.g. BIND, NSD, PowerDNS, Knot, include interfaces that make it possible to automate the transfer.

That’s the bad news. Here’s the good news.

1. Even without programmable interfaces, the necessary steps can be carried out manually. In 2009, when PIR was preparing to sign the .org zone, it asked for assurance that a registrant could sign his domain under one of the registrars and still be able to transfer the registration to another registrar if desired.

At the time, my group at Shinkuro, Inc., was part of a team under contract to the U.S. Dept of Homeland Security to facilitate the deployment of DNSSEC. We worked through the scenarios for accomplishing the transfers and demonstrated each of them. We didn’t include a change of registrant, so in terms of the table above, we covered scenarios 1 through 5. We further distinguished between DNS service that was provided by the registrar and DNS service that was independent of the registrar.
2. The old DNS operator is not always a “loser”

Changing the DNS operator involves three distinct steps:

* 1. The new DNS operator acquires a copy of the zone and puts it into operation. Both old and new DNS operators includes both sets of name servers in their list of name servers.
	2. The two DNS services remain in operation together for some period.
	3. The old DNS service ends, and the corresponding data is removed from the new operator’s zone.

If the zone is signed, then step (a) includes signing by the new operator and cross-sharing of the keys.

Step (b) must be long enough to make sure all the caching resolvers have updated copies of the list of name servers and, in the case of a signed zone, updated copies of the list of keys. The time required for this depends on the TTL (Time to Live) settings in the zone. Typical TTLs are 48 hours, and it may take a bit more time to be certain everything has settled down.

The above requirement determines the minimal amount of time for Step (b). What is the maximum time? There isn’t any. With both DNS operations running, the customer has the benefit of increased DNS service and increased protection against disruption of DNS service. With respect to DNS service, as opposed to registration, it is perfectly reasonable to have multiple DNS services. Therefore, instead of thinking only in terms of transferring DNS service from a losing operator a gaining operator, it is useful to think of the transfer as composed of two distinct and separable actions: (1) adding a new DNS operation; (2) removing a DNS operation. Step 1 is the same for initiating concurrent operation of multiple DNS services and for moving from one DNS operator to another. Thus, the existing DNS operator has at least some motivation to support this step to cooperate in providing the customer with the service they want.

1. There is active work underway to automate the multi-signer scenario. RFC 8901 documents the protocol steps, and a small consortium of companies is actively working on the design, implementation, and demonstration of software to fully automate the steps. This work is presented regularly at the DNSSEC Workshops during ICANN meetings. The project includes working with the major DNS software vendors to have programmable interfaces added to their software and augmenting the relevant RFCs to include the required functionality.

Here is a list of the panel sessions on DNSSEC Provisioning Automation at the last four ICANN meetings.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Date | Meeting | Presentation URLs |
| 1 | 11 Mar 2020 | ICANN 67 “Cancún” | <https://tinyurl.com/5dwxfz2v> |
| 2 | 22 Jun 2020 | ICANN 68 “Kuala Lumpur” | [xhttps://tinyurl.com/m8eraezu](https://tinyurl.com/m8eraezu) |
| 3 | 21 Oct 2020 | ICANN 69 “Hamburg” | <https://tinyurl.com/f8ma6347> |
| 4 | 24 Mar 2021 | ICANN 70 “Cancún” | <https://tinyurl.com/bj69sn87> |

 This is a continuing series. The next session will be on Monday, 14 June.

## Conclusion

It is worthwhile considering the full set of scenarios. It requires a bit of work, but much of that work has been done and is accessible.