

Applications for Resource Certification

Resource Transfers

r1.4 – 18 Jan 2008 – 11:47 – [DanielFKarrenberg](#)

Author: Robert Kisteleki

FIRST DRAFT !

Motivation

As the unallocated pool of IPv4 addresses run out there will be an increased incentive to those holding unused or under-utilised parts of the IPv4 address space to make it available to others who need such space. (Note: This discussion is independent of the economic or contractual modalities of such transfers or the registry policies governing them.) Certificates can help to make the transfers of address space assignments more reliable and secure by establishing that the seller side actually has the right to use the resources in question and that the rights can be transferred only once. Certificates can also help establish without doubt and delay that the receiving party is the new user of the resource.

Note: the current widespread terminology uses the terms "seller" and "buyer", so we'll stick to that even if it's not 100% appropriate.

Theoretically it is also possible to do IPv6 or AS resource transfers, since there is practically not much difference between IPv4 and IPv6/AS transfers in terms of process, interested parties or technical requirements. However, since depletion of these pools is currently not an issue, we'll concentrate on IPv4 resources only.

Business case

Approaching the depletion of the IPv4 space, these resources will become more and more precious. As some services do not (yet) work with IPv6, there is going to be a need for IPv4 addresses for a long time still. However, as the RIRs' pools run out, the only way to legally get more resources allocated is to buy them from an ISP that has some allocated but does not need it. This of course will usually be "carved out" from an existing larger allocation block.

Note: even though talking about the "price" of IPv4 resources is probably not appropriate, "value" might very well be.

Another reason for implementing resource transfers as a well defined and controlled process could be to avoid "RIR shopping"; ie. ISPs dealing with RIRs outside their original service region with the sole purpose of collecting more resources. Even though this will very probably not stop RIR shopping, it can make it less useful as a way of misusing the system.

Resource transfers with and without the help of resource certificates

We can easily imagine the resource transfer process in a world where no resource certificates exist:

- the buyer and seller find each other by whatever means, agree on the transfer of a resource
- they collectively contact their representative RIRs (or RIR, if they are in the same region) and notify them/it that they agreed on the transfer which now needs to be done at the registry level
- the RIR verifies the identity of the parties by whatever method it deems necessary. If the transfer happens in a cross-RIR fashion, one RIR has to rely on the other to identify its

member

- upon successful verification the RIR updates its internal database and (probably) to reflect the new situation and propagates these changes to its public database (WHOIS, IRR, etc.)

If resource certification is in place, the transfer process can be implemented by solely using this infrastructure (sometimes called **certificate driven transfer**):

- the buyer and seller find each other by whatever means, agree on the transfer of a resource
- they both sign a dedicated electronic document expressing their will to transfer a particular resource. The signature is made with the resource certificate itself, or, on the buyer's side, its identity certificate used in the resource certification context
- the signed electronic agreement can be sent to the RIR (if multiple RIRs are involved, then to the buyer's RIR)
- the RIR can automatically verify the agreement, as all the certificates used are either known to it or can be validated through the resource delegation chain
- once the automation RIR verified the transfer agreement, the relevant internal database change can be automatically made, which can be reflected in the public databases as well as in the resource certificate system – the buyer now has the right to ask a certificate over the resource, while the seller's now-overclaiming certificates are replaced with fitting ones

An advantage of this system is that it is fully automated, it does not need manual work or approval from the RIR. The disadvantage is almost the same: no policy or other decisions, double checks can be applied.

The middle ground between the above two solutions can be the following:

- the transfer is initiated the same way as with the certificate driven process, but
- the agreement validation process does not cause an automatic update in the RIR internal database – instead it pops up as a ticket for the hostmasters, with a "green light" indicating that the parties are already identified and they provided proof that they want to enter into this transaction
- the hostmaster can have the ultimate power to authorize, hold or deny the transaction based on further inputs like:
 - the policies that apply to that specific resource
 - member (financial or other) status of the buyer/seller: for example no one should be allowed to buy/sell a resource if they are not a member in good standing
 - any other checks that the community sees fit
- upon accepting the transaction, the relevant internal database changes are made, which are again reflected in public databases and in the resource certification system.

The advantage of this approach is that it saves the RIR from most of the manual work of validating the transaction (since that can be done automatically) while allowing to do manual checks too. Another advantage is that this approach avoids automatic, externally triggered internal database changes, thereby eliminating an attack vector against the RIR database.

Detailed operation

Whenever a resource transfer transaction is about to take place, the following assumptions hold:

- The resource to-be-transferred is one that originally comes from one specific RIR. In case this is not true (ie. the resource is a range that spans through multiple authoritative RIRs), the resource should be split on RIR boundaries and transaction should be looked at two (or more) independent transactions.
- The seller is a member of an RIR and, for that particular resource, has a well defined resource delegation path that originates at this RIR. This delegation path might include several entities along the delegation chain.
- The buyer is a member of an RIR (preferably the same RIR as the seller, but it doesn't have to be the case – see below), and already has its contractual/technical background to receive and use certificates for its resources.

Based on the above, the following steps are needed to handle the transaction:

- The buyer and the seller agree on a "swing point" in the resource certification hierarchy. The "swing point" is an entity that is trusted by both the buyer and the seller and that is a common ancestor of the buyer and the seller. Note that there is **always** such an entity – the

- authoritative RIR, if nobody else.
- The buyer, the seller and the swing point enter into a locking mechanism for that resource:
 - the swing point hands out a kind of "document to be signed by the parties" to the buyer and the seller
 - the swing point promises that the resource is locked in the sense that until the current transaction succeeds or fails, it will not modify the resource's allocation in any way
 - the swing point promises that if the transaction succeeds, then the resource will be transferred from the seller to the buyer meaning:
 - the resource is revoked from the seller, and all certificates the seller has containing that resource will be revoked/reissued with that resource excluded
 - the resource is allocated to the buyer, and from this point on the buyer is eligible for a certificate over it
- By definition:
 - the transfer succeeds if both the seller and the buyer sends back the "document" specified above, in signed form
 - the transfer fails if up until a predefined time the swing point does not receive both signatures. In this case the locking over that resource is completely cleared.
- The swing point is not involved in any other aspects of the transfer, such as price/conditions negotiations, money transfer, liaising, etc. Its purpose is purely technical. This helps keeping the swing point unbiased.
- Technically, entities above the swing point in the hierarchy do not have to be involved with the transaction. Policy-wise, they might be.

The locking and "signed document" mechanism allows to:

- make sure that the seller cannot sell the same resource to multiple entities
- make sure that the buyer will receive the resource once the transaction has taken place

Note: there might be intermediary entities between the seller and the swing point or the buyer and the swing point. In this case the resource transfer lock has to be applied to these intermediaries too.

In other words, some of them also have to make promises:

- Intermediate entities on the seller's chain are not of huge importance as the certificate as they participation in not directly needed. Still, they should know about the transaction in order to avoid using out-of-date certificates.
- Intermediate entities on the buyer's chain have to make commitments to delegate the resource down to the buyer, once they receive it from their issuer. This is to ensure that the resource bought/sold does not end up stuck at some such intermediary point.

It's clear to see that if the swing point is not the common ancestor (upstream, CA, IR, ...) of buyer and seller, then the situation is much more complex: policy-wise, technically, operationally, legally, financially, "everything-ally". No wonder that the design group is trying to refrain from specifying this.

The above process can handle the case if the buyer and the seller are in different regions: the resource "cross-certification" between the RIRs solves this. The buyer will receive the resource through a delegation path that includes its own RIR. The path itself end at the origination RIR, which is another good incentive for the relying parties to use the "natural" trust anchors (RIRs) when validating certificates.

Related issues

Transfer of live networks

It is anticipated that during a transfer process most of the resources need to be "kept alive", ie. there has to be a valid certificate for the at all times, otherwise the routing of the resource might stop. In other words, to be on the safe side in terms of network availability, the transfer mechanism should support a "make before break" approach – one that almost contradicts the ability to prevent the multiple sale problem. Details have yet to be figured out.

Split/merge case

Organization splits and merges can be considered as special cases of resource transfers.

During a split, a new entity is created, which originally has no resources, but can "buy" some from the original entity. From the swing point's point of view, this is no different than from a regular transfer.

If two organizations merge, the resources from one have to be transferred into the resource set of the other. Again, from the swing point's point of view, this is just a regular transfer.

Liability issues, notary role

One has to note that when introduction resource certification, the role of an internet registry (RIR, LIR, NIR, ISP, anything that acts as such) might change. As per today, if there is a human error during the allocation (or, there's an abuse of the registry system) it can be corrected, and no real harm is done. However, when certification is in place – especially if dealing with transfers – this can lead to network outages multiple sales/purchases of the same resource, etc., which can cause significant financial damage to the involved parties. This opens up a threat that the IRs did not have to deal with before, one that the IRs naturally want to avoid.

This leads to a need to reinforce the IRs "notary role": even with certification, the IRs should not be financially liable for the transactions they handle – they are only registering the changes. This is a far fetching question, which has not yet been discussed in every detail.

Revision: r1.4 – 18 Jan 2008 – 11:47 – [DanielFKarrenberg](#)

[Science](#) > [CertWhitePapers](#) > [CertWhitePapersTransfers](#)

Copyright © 1999–2008 RIPE NCC.