Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 1, 2015

R. Austein
Dragon Research Labs
R. Bush
IIJ Lab / Dragon Research Lab
G. Huston
G. Michaelson
Asia Pacific Network Information Centre
May 30, 2015

Resource Transfer in the Resource Public Key Infrastructure
draft-ymbk-sidr-transfer-00

Abstract

Transfer within the RPKI of actual address space and/or autonomous system number resources between two Internet registries (ISPs, RIRs, NIRs, etc.) is reasonably achievable for most useful operational needs. In this paper, we describe, at a high level, how this may be accomplished.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 1, 2015.

Copyright Notice

Table of Contents

1. Introduction and Terms

To paraphrase the Introduction of [RFC6480], the "Resource Public Key Infrastructure (RPKI) represents the allocation hierarchy of IP address space and Autonomous System (AS) numbers; and is a distributed repository system for storing and disseminating the data objects that comprise the RPKI, as well as other signed objects necessary for improved routing security."

An Internet Registry (IR) is the IANA, a Regional Internet Registry (RIR), a National Internet Registry (NIR), a Local Internet Registry (LIR), a Internet Service Provider (ISP), or an end site which may hold IP resources and is the subject of one or more certificates using [RFC3779] extensions in the Resource Public Key Infrastructure (RPKI), see [RFC6480].

It is desirable to transfer resources between resource-holding entities in the RPKI, and to do so without violating contracts, policies, etc., and while maintaining operational reliability and administrative accuracy with minimal administrative overhead.

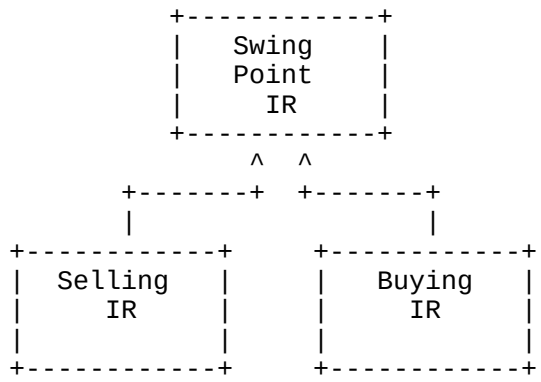

Fig 1. The Simplest Example of Seller, Buyer, and Swing Point

Seller and Buyer are used to describe the end parties to a transfer, the selling IR transferring the resource(s) to the buying IR. For the purposes of this document, the terms seller and buyer are used, although layer nine considerations may require less commercial formal roles.

Transfer is the sale and corresponding purchase of literal address space or autonomous system numbers between two parties. The seller relinquishing some amount of resource and the buyer being allocated a similar amount but not the same literal address space, is not a transfer, and is not further considered here.

A Swing Point is the IR at the lowest point in the RPKI hierarchy which the seller and buyer have as a common parent and which has agreed to be used as the agent of transfer.

While there is no automated method for the RPKI to assist the parties to a transaction in determining that all business and policy aspects of a transaction are satisfied, these layer eight and nine issues can be resolved using normal business practices.

2. A Simplistic Case

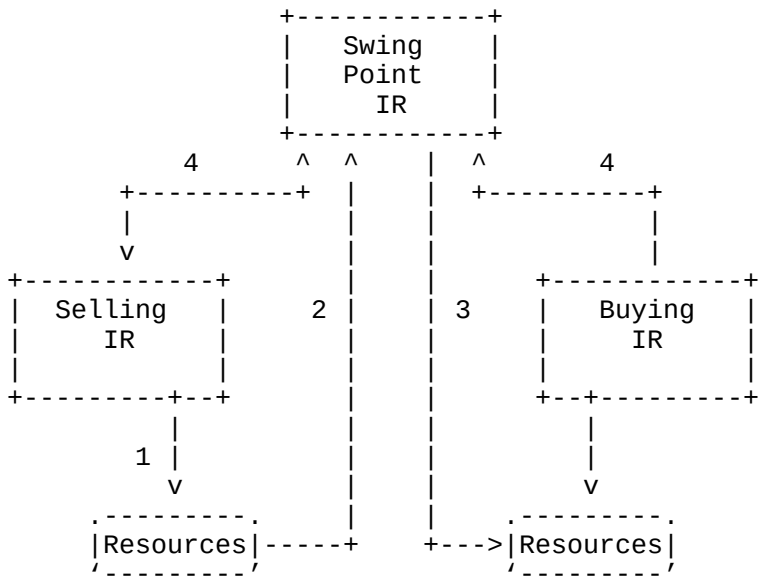

Fig 2. Steps in a Simple Transfer

2.1. Steps in Simple Case

As a formal business relationship between all parties to a transfer provides a level of trust which allows simple transactions, we first consider the simple case where the seller and the buyer are both directly known to the swing point, see Figure 1.

The transfer is done in the following steps (see Figure 2):

1. The seller creates a certificate describing the subset of the seller's resources which are to be transferred.
2. The seller tells the swing point that it wishes to transfer the resources described by the certificate to the buyer.
3. The swing point issues a new expanded certificate to the buyer describing the buyer's old holdings plus the new resources.
4. When the seller and the buyer are comfortable that both the technical aspects (customers swung, routing done, etc.) and the business aspects of the transfer have been accomplished, they inform the swing point which then shrinks the seller's resource certificate, removing the transferred resources.

2.2. The Torn Euro Protocol

Due to issues of cancellation, reneging, and fraud, step 4 above, where the seller and the buyer tell the swing point that the deal is done, needs to be formal in some fashion. For this purpose, we

envision a yet to be described torn Euro protocol, where the buyer and the seller each hold one half of a virtual torn Euro note, and the swing point believes the transaction to be complete when it has received both halves and they match.

This protocol has yet to be described, and Steve Kent has taken on the task of looking for an existing simple example that can be borrowed for the purpose.

3. A More Complex Case

What happens when the seller is not a direct customer of the swing point, see Figure 3.

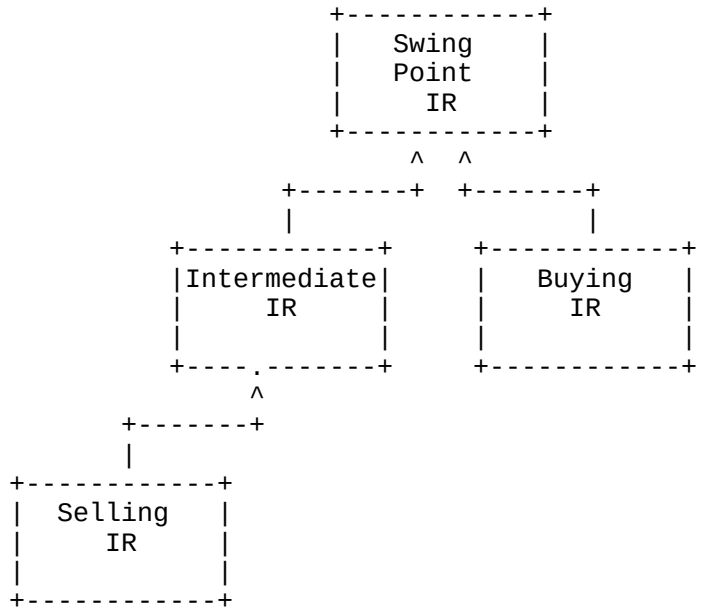

Figure 3. The Case of The Indirect Seller

The swing point needs to be assured that it is contractually able to move the resource given its relationship to the Other IR. As RFC 3779 extensions do not codify business issues such as PI/PA, and rights to resell, this has to be handled out of band, there is no way to automate it. But this is part of today's IR address space management process and will continue to be handled manually.

Therefore the process is the same as for the simple case, except that, before issuing the expanded certificate to the buyer in step 3, the swing point must assure itself that policy and contractual issues are cleared. It might be well-advised to contact the intermediate IR

and gain its consent, possibly with the assistance of the seller. The bottom line is that the swing point does own/control the resource being transferred, and therefore has the prerogative to act within its perception of the liabilities it is incurring.

This freedom allowing the seller to be indirectly related to the swing point may be induced to more levels of indirection. It is the swing point's obligation to perform diligence on the iterative financial, contractual, and policy obligations of the relationships down to the seller. Unfortunately, the RPKI can not automate this.

3.1. The Indirect Buyer

The case where the buyer is not directly known to the swing point is more difficult. Among other issues, the buyer may not be an existing resource holder at all, i.e. there may be no path down from the IANA root to the buyer. In this case, the buyer must explore the graph and choose an IR with which to contract a relationship. This can be both a business issue and a policy issue, e.g. can a buyer in Asia choose a parent which is, directly or indirectly, an ARIN customer?

The case where the buyer contracts directly to become a customer of the swing point has been explored above. What if the buyer becomes a grandchild of the swing point, as in figure 4?

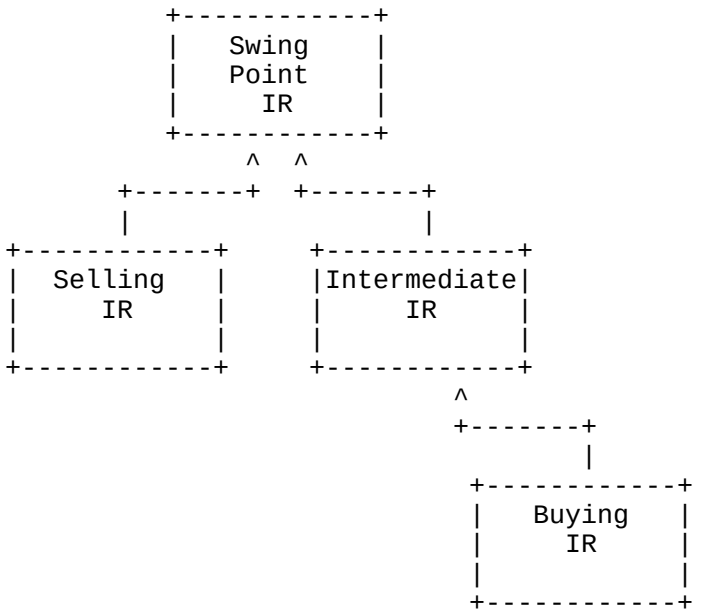

Figure 3. The Case of The Indirect Buyer

Somewhat analogously to the case of the indirect seller, the swing point has to iteratively verify that the IRs between it and the buyer are all willing to contractually and technically accept the resource(s) to be allocated to the buyer. But, in the case of the indirect buyer, the iterative conditions are much stronger. In the indirect seller case, the swing point has contractual control of the chain between it and the seller. In the case of the indirect buyer, all intermediate IRs between the swing point and the buyer must give business and technical consent. The swing point can not force its child to issue a resource certificate to the buyer.

Things may not be as bad as they appear at first blush. The buyer is actually contracting to its parent, and part of that contract will presumably be that the parent agrees to issue the resource certificate to the buyer when it receives the resource from it's parent. And this presumably applies to the buyer's parent's relationship to a grandparent and so forth. On the other hand, the swing point has no mechanical way to test the willingness of the IRs on the buyer's indirect chain. But the swing point can know when the buyer is happy that it has received the resources, as the buyer will give it the buyer's half of the torn Euro.

3.2. The Difference Between Buyer and Seller Chain

Essentially, the difference between an indirect buyer chain and an indirect seller chain is that the swing point has the logical, though maybe not contractual, prerogative to pull address space from the seller's chain, but does not have the power to push it down the buyer's chain. All IRs on the buyer's chain must agree to certify downward toward the buyer.

4. Transfer in the Absense of a Common Ancestor

For political reasons, the current RPKI structure has no single root trust anchor. There are a number of roots, e.g. the five RIRs who do not descend from the IANA. This creates considerable complexity and some risk for resource transfers between entities without a common ancestor.

To work around this problem, each RIR certifies a subsidiary Certificate Authority for each other RIR to which it transfers resources, see Figure 4, and issues the transferred resources to that subsidiary CA.

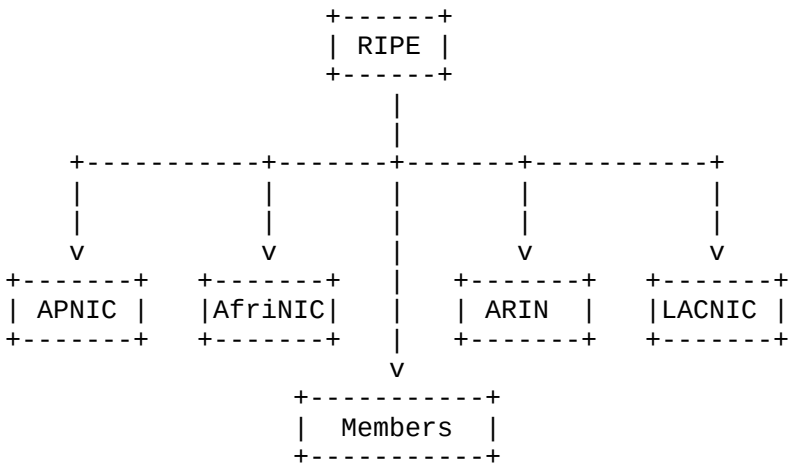

Figure 4: The RIRs each certify proxy CAs
for all of the other RIRs.

But, to use the example of Figure 4, the APNIC CA to which RIPE issues resources is, in fact, run by APNIC under APNIC's Business Certificate PKI (see [RFC6492] Section 3) and uses an APNIC-provided publication point.

Thus APNIC has under its control, among other things, four CAs, one with resources from each of the other CAs. And similarly for each of the other RIRs.

So the swing point for a transfer from an APNIC member to a RIPE member is the APNIC CA. And an APNIC member holding resources originated by APNIC as well as resources transferred in from another RIR, e.g. RIPE, actually holds two resource certificates.

This could probably be made more complicated and brittle, but it would require serious effort.

5. Transfer in process: Resources Change Forced from Above

Even though both seller and buyer have agreed to a transfer, the seller might try to not relinquish the resource, hoping to sell it more than once. Therefore it may become necessary to force closure for a non-compliant seller. In this case, a resource holding would be changed, shrunk, by force from above.

A 'normal' (i.e. what the RPKI design anticipated) resource shrinkage is initiated by the leaf resource holder and propagates upward toward

the root of the tree. At no point in this process does a holder claim more than their parent believes they have.

When a resource is forcibly removed from 'above', the shrinkage propagates downward. Until the ultimate holder relinquishes the resource, at some point in the path down the tree a child holds more resources than its parent believes it does. As the protocol model is bottom initiated polling, see [RFC6492], the time window of exposure of this over-claiming can be relatively large.

6. Security Considerations

Ghu only knows.

7. Acknowledgements

Thanks Mom!

8. IANA Considerations

Nothing is required of the IANA; though it would make some things a lot simpler if the IANA was the root TA/CA of the entire tree.

9. References

9.1. Normative References

[RFC6492] Huston, G., Loomans, R., Ellacott, B., and R. Austein, "A Protocol for Provisioning Resource Certificates", RFC 6492, February 2012.

9.2. Informative References

[RFC3779] Lynn, C., Kent, S., and K. Seo, "X.509 Extensions for IP Addresses and AS Identifiers", RFC 3779, June 2004.

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, February 2012.

Authors' Addresses

Rob Austein
Dragon Research Lab
40 Gavin Circle
Reading, MA 01867
USA

Email: sra@hactrn.net

Randy Bush
IIJ / Dragon Research Labs
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com

Geoff Huston
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
AU

Email: gih@apnic.net

George Michaelson
Asia Pacific Network Information Centre
6 Cordelia St
South Brisbane, QLD 4101
AU

Email: ggm@apnic.net