

Applications for Resource Certification

More Automatic Provisioning

r1.3 – 18 Jan 2008 – 11:42 – [DanielFKarrenberg](#)

Authors: Robert Kisteleki, Daniel Karrenberg

Business Case

Currently there is no convenient and automatic way to make sure that a particular AS is authorised to announce or originate a certain prefix, i.e. that

- the prefix is really in use, and
- the legitimate user of the prefix authorises a specific AS to announce that prefix.

This means that all responsible ISPs will spend some people resources to search various allocation and routing databases to make sure that a customer presenting a prefix for routing is actually the legitimate user of the address space; many higher tier providers also have similar procedures in place to verify the routes that their transit customers are presenting. This practice has a number of problems:

- It takes skilled engineers to execute the heuristic checks required.
- The process cannot be fully automated so it is time consuming.
- The process does usually not check frequently whether the originally verified authorisation still persists.
- Many routing registries have little safeguards in terms of who is authorised and able to insert information into them; also, human error in such registries can add to the confusion.
- Fear about competitors not checking as thoroughly as oneself may cause checks to be less than thorough.

If these checks could be automated in a dependable and transparent way, they stand a good chance to be more widely applied. This would result in less chances of address hijacking or routing instabilities caused by intentional or erroneous misconfiguration.

Automated provisioning makes the checks not only repeatable and more stable, but cheaper for the ISP. Might cause ISPs to prefer customers with certified resources and/or make such services slightly cheaper if such a certification can be presented by the customer.

Principle of Operation

Internet resource certificates can help to achieve a high degree of automation here. It would work roughly like this:

- Prefix holders will be able to obtain a certificate over their prefixes. These certificates are verifiable by an automated process, which gives the ISP a confirmation of their validity: if they can be "traced back" through a chain of issuers to a known trusted point (trust anchor in PKI terms), then the certificate is valid and acceptable, therefor the resources contained therein are valid and usable.
- The prefix holder, using their certificate over a particular prefix, can sign a so called Route Origination Authorization (ROA), which is essentially document saying roughly the following: *"The holder of the prefix A/B hereby authorizes the operator of ASxy to announce the prefix. This authorization is valid until it is explicitly revoked, or at most until YYYY-MM-DD."* This document is digitally signed using the certificate in question. If the prefix holder is able to produce such a signed document and the signature, which can be automatically checked, turns out to be fully valid, then the ISP can have the highest assurance of that claim being valid.

- Similarly routing requests to transit ISPs could be made by documents digitally signed by the originating AS using a resource certificate over their AS number resource. The ROA and this document in combination are sufficient proof to the upstream provider of the originating AS that this is a legitimate route to accept.
- The documents mentioned above could be stored in repositories which are accessible to the ISPs.
- Since the above checks are (can be) automated, it's easy to do them periodically. This reduces the risk of maintaining a service that has no legitimate background any more.
- Transitive

Illustrations

We need to do some illustrations showing the actions and information flow for this application.

Conclusion

Even without secure routing protocols deployed and in widespread use, address space and AS certificates can make Internet routing more secure and stable by making the provisioning process more secure and providing a means to check periodically whether the authorisation to originate and propagate a specific route still exists. The success of such automated provisioning can also serve as a confidence builder among ISPs if secure routing protocols should become necessary in the future.

Revision: r1.3 – 18 Jan 2008 – 11:42 – [DanielFKarrenberg](#)

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

Copyright © 1999–2008 RIPE NCC.