Resource Public Key Infrastructure (RPKI)

“A tradeoff between security and freedom”

The Resource Public Key Infrastructure (RPKI), also known as Resource Certification[[1]](#footnote-1), is a security framework for verifying the association between resource holders and their Internet resources. The Internet resources are the Internet Protocol (IP) addresses and Autonomous System (AS) numbers. The RPKI is also believed to make the registry’s more robust and reliable and Internet routing more secure by securing the BGP routing process.

As stated in RFC6491 (2012), the RPKI was designed to provide a secured way to ascertain the holder of IP addresses and AS numbers. Within its framework, a relying party can assess the validity of routing information. One instance is route origin validation to detect IP prefix hijacks, by mistake or on purpose. It is up to the network operator to define local policies and the actions that are taken on valid/invalid/unknown status of a route announcement.

Certificates issued under the RPKI contain attributes that identify IP addresses (IPv4/IPv6), and Autonomous System number resources, see RFC6480 (2012) for more details.

The main advantages that the RPKI is believed to offer are as below:

1. Prevention of deliberate and unintentional routing problem
2. Enabling more flexible and efficient use of address resources
3. Reducing chances of having their resource hijacked by malicious users
4. Reducing effect caused by router configuration error
5. Centralizing power – Easier control and monitoring
6. Facilitation of smooth transfer of IPv4 address resources from one party to another
7. Use of dedicated End Entity certificate to verify each objects automatic expiry

However, if RPKI is used there are concerns that could affect the growth, freedom and democratic process that the Internet currently enjoys. Some of these concerns are highlighted below:

1. The RPKI can be used to Revoke certificates and has raised user concerns on length of certificate expiry and revocation procedures that will have direct operational effect.

Until now, it was only the Domain names that could have been revoked or taken back by respective resource owners, as in the case of unilateral action by U.S government against www.rozadirecta.com in the recent past but, IP address were fairly independent of any such unilateral actions. With the introduction of the RPKI, the IP addresses could also be subject to such unilateral actions by resource owners that could enable the Internet address registries, and origin of resources in possession of the RPKI keys, to unilaterally take back the IP address at their discretion. It can be misused for financial gains or other favors that will drastically impact the freedom and democracy, the very foundations of the Internet. The Autonomy of the ISP’s and sovereign states will be compromised and marginalized to a large extent, as RPKI will give RIRs direct operational impact on routing.

1. Financially, it may be an expensive proposition as the routers & software’s used by ISPs and the organizations that use BGP protocol would need to be upgraded.
2. Finally, it will further centralize control over the Internet in the hands of few, intensifying political struggle and possible chances of the Internet fragmenting.

Even more concerning is the fact that since last year the project has been in full swing but very little has been known about its progress, and the public participation has been virtually non-existent.

As it appears now, “a test-bed has been active since last year, which is based on the rpki.net software package and allows network operators to install, configure, and experiment with RPKI. Besides the rpki.net software, two major router vendors, Cisco and Juniper, have made available software images for some of their routers such that validation can be used in routing policy definitions. SURFnet, a Canadian research alliance of academic researchers, industry partners, and government collaborators were amongst the few to have participated in this test-bed (Jac, François, and Benno, 2011).

The current structure of the Internet is already hierarchical and the implementation of RPKI could further strengthen this hierarchy of control and centralize power.

Although the RPKI undoubtly has some merits, the tradeoff in comparsion to what it has to offer is huge! It is therefore imperative now that the Internet users of the world, in the larger interest of the Internet and its expansion to the bottom billion, places an objection to this project and have it absolved before implementation. It’s time to bring this issue into larger public discussion forums to create more awareness on the true implications of RPKI.

**References**

Lepinski, M., & Kent, S. (2012A). An Infrastructure to Support Secure Internet Routing. RFC6480. Internet Engineering Task Force. Retrieved from http//tools.etf.org/html/rfc6480

Manderson, T., Vegoda, L., & Kent, S. (2012B). Resource Public Key Infrastructure (RPKI) Objects Issued by IANA. RFC6491. Internet Engineering Task Force. Retrieved from http//tools.etf.org/html/rfc6491

Huston, G., & Bush, R. (2011). Securing BGP and SIDR (online). Retrieved from ……..

Jac Kloots, François Kooman, and Benno Overeinder (2011). Resource PKI (RPKI): Design and Operation of the Infrastructure. Retrieved from http://www.surfnet.nl/nl/Innovatieprogramma's/gigaport3/Documents/FIP-11-02%20Routing%20Security%20D02-1.pdf

Geoff Huston and Randy Bush. IETF Journal Volume 7, Issue 1(July 2011), Securing BGP and SIDR. Retrieved from http://isoc.org/wp/ietfjournal/?p=2438#more-2438

IAB statement on the RPKI. Retrieved from http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html

Presentation on Resource Certification (RPKI) by Alex Band, product Manager RIPE NCC. Retrieved from http://www.dknog.dk/dknog2/presentations/RPKI\_DKNOG.pdf

Geoff Huston, George Michaelson and Stephen Kent. Resource Certification - A Public Key Infrastructure for IP Addresses and AS's. Retrieved from http://www.potaroo.net/papers/2009-12-ieee-glow09/rpki-2009-08.pdf

1. http://en.wikipedia.org/wiki/Resource\_Public\_Key\_Infrastructure [↑](#footnote-ref-1)