# Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing

**Brenden KUERBIS & Milton L. MUELLER**
Syracuse University, School of Information Studies

***Abstract:*** New security technologies are never neutral in their impact; it is known that they can alter power relations and economic dependencies among stakeholders. This article examines the attempt to introduce the Resource Public Key Infrastructure (RPKI) to the Internet to help improve routing security, and identifies incentives various actors have towards RPKI implementation. We argue that RPKI requires ISPs to achieve security at the expense of autonomy, requires all actors to tradeoff simplified global compatability and centralization of power, and affects the policies and business models of the Regional Internet Registries and their relationship to the Internet Corporation for Assigned Names and Numbers. While the Internet remains a space where authority is highly distributed, elements of hierarchy do exist, especially around critical resource allocation, and it is likely that security and other concerns will lead to continuing efforts to leverage those hierarchies into more powerful governance arrangements.

***Key words:*** routing, internet addresses, security, RPKI, ICANN, Regional Internet Registries, ISPs.

Routing and addressing are at the core of how the internet works. Every second, routing arrangements must be able to successfully move trillions of individual data packets from any originating network in the world to any one of millions of destinations anywhere in the world. Some of the most important cybersecurity problems relate to the way networks acquire address blocks and exchange routing information among each other. Efforts to solve routing-related security problems reveal how complex and difficult it can be to attain global acceptance and implementation of security-enhancing standards and practices.

The original Internet routing protocol assumed that all routers in all networks were trustworthy. Today, the existence of malicious actors on the Internet is a given. Additionally, the routing infrastructure is vulnerable to unintentional misconfigurations that can cause harmful results. (ENISA, 2010; BARBIR, MURPHY & YANG, 2006) One security flaw was illustrated

vividly in 2008 when a Pakistani ISP's attempt to block YouTube within their country propagated false routing information to ISPs around the world, effectively knocking YouTube off the Internet for a short period. [1] Several other well known misconfigurations that led to temporary routing outages have occurred in the past, although the overall extent and severity of the routing security problems network operators' deal with is not empirically documented in any publicly accessible, systematic way. The perceived need for greater security in routing has led to an attempt to create a Public Key Infrastructure for Internet protocol addresses and routes. Resource Public Key Infrastructure (RPKI) is a security technology that would create a hierarchy of digital certificates which would be used to authenticate both the holder of address blocks and the origination of route announcements using those blocks.

This paper begins with the premise that implementations of security technologies are never neutral in their impact; they alter power and economic relations and raise strategic and policy issues. (ANDERSON & MOORE, 2006) This is particularly true with the internet, where the interdependence of many autonomous, diverse stakeholders can make it especially difficult to devise effective security solutions. (BAUER & VAN EETEN, 2009) This paper considers two research questions generated by that theory. First, what kind of shifts in power relations and cost-benefit distributions are produced by efforts to make Internet routing more secure using RPKI? Once these reconfigurations have been identified, one can then understand the incentives various actors have towards RPKI implementation. This leads to our next research question: is the implementation of RPKI facilitated or impeded by those incentives? In other words, are its prospects for implementation good, or will its adoption likely be blocked due to the unwillingness of actors to accept the power shifts and altered economic distributions?

In the next section, we briefly describe the prevailing state of internet routing. After that, we describe how RPKI proposes to solve these problems using digital certificates to bind IP address blocks issued by the extant allocation hierarchy to ISPs and internet routing information. The next section analyzes the ways in which RPKI produces shifts in power relations and cost-benefit distributions. In the concluding section we summarize our findings.

---

[1] See http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

## ■ Routing and security

Routing is the automated process that directs Internet protocol packets from their origin to their destination. IP addresses can be described as part of the language that routers speak to each other. Internet routing protocols consider the IP address to be composed of two parts: the address of the network (the prefix) and the address of the connected computer (the host). Routing through the Internet is based on the network portion of the address. For each prefix, a router stores information telling it how to find a path to it and uses this information to construct a forwarding table (the routing table) that controls the movement of each incoming packet to the next hop in its journey. Routers also transmit announcements to other routers about the address prefixes to which it is able to deliver packets, and this information is incorporated into the tables of other routers. Thus, routers are engaged in constant, automated conversations with each other that exchange network prefixes and other routing policy information to keep every router informed about how to reach tens of thousands of other networks on the Internet.

Currently, interactions among routers are based on an Internet standard known as Border Gateway Protocol (BGP). As originally described in RFC 1771 (1995), and as later updated by RFC 4271 (2006), BGP is the dominant inter-domain routing protocol of the Internet (REKHTER & LI, 1995; REKHTER *et al*., 2006). As noted earlier, the original BGP protocol assumed that all Autonomous Systems (ASes) were trustworthy. As the Internet grew, the assumption of ubiquitous trust made less and less sense (HU, McGREW *et al*., 2006). Extensive work has been done in the technical community exploring the issue of routing security and proposing various solutions to improve it (BUTLER, FARLEY, McDANIEL & REXFORD, 2010).

Some assessments of this problem are more alarmist than others. Some observers ridicule the existing state of affairs as "routing by rumor" (Internet Architecture Board [IAB], 2010) and emphasize the fragility of the whole system (BUSH, AUSTEIN & BELLOVIN, 2010). Other voices are less alarmed. They note that a variety of measures are already in place by ISPs to filter out false route announcements. They claim that the same network operators who don't currently filter BGP announcements properly are not likely to deploy new security solutions such as RPKI. A major breakdown such as the Pakistan case, they claim, applied only to one site and was remedied in about two hours; routing takes place reliably in the vast majority of cases.

## ■ RPKI as a proposed solution

RPKI uses digital resource certificates to authenticate the possession and use of IP address blocks, Autonomous System (AS) numbers, and route announcements. (KENT, 2006) Certificates bind a resource holder of IP address block prefixes to its public cryptographic key and possibly other information like Autonomous System (AS) numbers that have been allocated to the organization. Subsequently, resource holders can create route origin authorization (ROA) statements, or standardized verifiable attestations that the holder of a certain prefix authorizes a particular Autonomous System (AS) to announce that prefix. Using these certificates and ROAs, network operators (e.g., ISPs) can validate that 1) a specific network, as indicated by a unique AS, is the legitimate holder of an IP address block, and 2) the AS that originates a route announcement using a particular prefix is authorized to do so. Like all PKIs, authenticating certificates therein (and subsequently the associated allocation and routing information) would rely on the system having one or more Certification Authorities (CAs) [2], which could publish a public key(s) or "trust anchor" to be used to authenticate other certificates.

The Secure Inter-Domain Routing (SIDR) Working Group of the Internet Engineering Task Force, which was initiated in November 2005, produced an architectural specification for a Public Key Infrastructure for validating address holders, AS numbers and route authorizations. The critical feature of the proposed RPKI solution is the attempt to link resource certificates to the institutions that issue internet resources, namely ICANN and the RIRs. [3]

As Figure 1 shows, IP address resources are allocated and assigned on a hierarchical basis. By virtue of its U.S.-government granted contract to perform the Internet Assigned Numbers Authority (IANA) function, ICANN sits at the top of the delegation hierarchy. It makes large delegations (usually

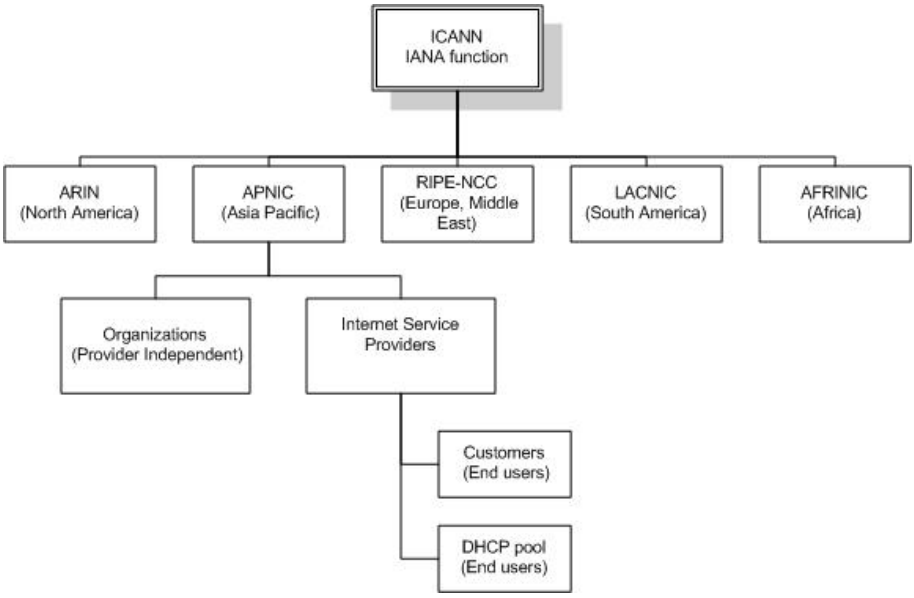
---

[2] Most users are familiar with digital certificates through their use of Certification Authorities (CAs) for web sites. CAs are third parties who are trusted by the subject (publisher) of the certificate and the parties interacting with the subject who rely upon the certificate for authenticating it (the relying party). This allows relying parties to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. Many private sector companies offer CA services commercially. Government agencies may also act as CAs, or organizations can set up their own, internal CA. A 2009 market share report determined that VeriSign and its acquisitions (which include Thawte and Geotrust) have a 47% share of the certification authority market, followed by GoDaddy (23%), and Comodo (15%). See Wikipedia http://en.wikipedia.org/wiki/Certificate_authority.

[3] See *An Infrastructure to Support Secure Internet Routing*. http://tools.ietf.org/html/draft-ietf-sidr-arch-11.

one or more /8 blocks of about 16.7 million individual IPv4 addresses) to the Regional Internet Registries (RIRs). The five RIRs, each roughly corresponding to a recognized geographic region, receive applications for addresses from Internet service providers, hosting services, and corporate networks within their region. The RIRs assign a unique Autonomous System Number (ASN) to each recipient and delegate address blocks to each AS based on technical need criteria. Internet service providers and organizations in turn sub-delegate address blocks to their customers or departments, respectively. The SIDR working group proposed that the RPKI mirror this delegation hierarchy. It did so because, in its own words, "existing resource allocation and revocation practices have well-defined correspondents in this architecture." [4]

**Figure 1 - IP address allocation hierarchy**




In a February 2010 official statement, the Internet Architecture Board (IAB), the chief supervisory body of the IETF, expressed its support for the linkage between the trust anchor hierarchy and the address allocation hierarchy:

[4] See Section 1 of *An Infrastructure to Support Secure Internet Routing*. The statement was partly inaccurate because there are few established practices and few precedents for resource revocation in current policies.

> "The IAB considers a properly designed and deployed RPKI to be an absolute prerequisite to having a secure global routing system, which is in turn a prerequisite to having a reliable worldwide Internet. ... The SIDR architecture and protocols have been designed to support a single trust anchor as well as multiple trust anchors. The IAB however, [believes that]: 1. the RPKI should have a single authoritative trust anchor; 2. this trust anchor should be aligned with the registry of the root of the allocation hierarchy." (IAB, 2010)

We now examine the way actor incentives interact in the current institutional environment. Implementation of RPKI depends on the actions of four distinct classes of actors: internet service providers (ISPs), the Regional Internet Registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN) [5], and the US Government. The actions of these globally distributed entities are not centrally coordinated or subject to any single hierarchical authority.

Below, we identify and briefly analyze four distinct ways in which RPKI's design and implementation shift power relations and cost-benefit distributions. The four points are:

- RPKI requires ISPs to trade off security and autonomy
- RPKI requires all actors to trade off simplified global compatibility and centralization of power
- RPKI affects the policies and business models of the RIRs
- RPKI affects the RIRs' relationship to IANA

***The incentives of ISPs: trading autonomy for security?***

ISPs are the most important and the most numerous set of actors. Their routing operations are the place where RPKI must be implemented if routing is to be secured using this technology. This class of actors includes not only large commercial service providers who sell internet access on the retail and wholesale level, but also thousands of private sector organizations that run their own networks and thus acquire address blocks. There are approximately 35,000 distinct autonomous systems connected through the global Internet.

[5] ICANN is a nonprofit corporation formed in 1998 to serve as the coordination and policy making institution for Internet domain names and IP addresses. It is a U.S. government-shepherded evolution from the Internet Assigned Numbers Authority (IANA) operated by Jon Postel at the Information Sciences Institute with support from other early Internet developers.

ISPs have mixed incentives to adopt such a technology. On the positive side, a generalized capacity to authenticate route announcements and address block holdings could provide a more efficient, more automated method for handling routing information in a secure way. At its best, RPKI would not only help to prevent bogus route announcements and address hijacking, it would also facilitate the smooth transfer of ipv4 address resources from one party to another after the free pool is depleted. A fully functional, globally compatible RPKI system would act as an effective property title for IP address blocks, giving the address holder legitimate claim to acquire or transfer address resources, and allow third parties to verify legitimate holders of addresses.

There are however externalities in the adoption and implementation of RPKI. As other literature has recognized, network externalities – or what has more accurately been termed demand-side economies of scope (ECONOMIDES & WHITE 1994; MUELLER, 1997) – can act as both facilitators and obstacles to security technology adoption (LELARGE, 2009). ISPs can only reap security benefits when its digital certificates for routes are reciprocally recognized by at least one other ISP. At a minimum, a pair of ISPs can achieve minimal security improvement by agreeing to authenticate each other's route announcements. The scope of the security increases as more ISPs join in a compatible network of certificate exchange. These network externalities have many of the features of a two-way network as defined by Economides (ECONOMIDES, 1996, p. 675), in that there is a distinction between originating a route and accepting a route announcement from another ISP. Because this scope can be widened incrementally, through pairwise agreements among ISPs, and still deliver some benefits with each additional partner, network externalities by themselves do not seem to pose an insurmountable hurdle to RPKI adoption.

But a universal RPKI regime that is tightly bound to the authoritative IP address allocation hierarchy does raise some serious risks for ISPs. If ISPs are required to obtain a certificate for their existing address blocks, there is a risk that the issuance of a certificate could be perceived as requiring a new assessment, by the RIR, as to whether the ISP qualifies for the address blocks it already has. [6] The ISP would have to pay careful attention to the

[6] In the ipv4 space, where the RIRs issued most of the allocations years ago, the RIRs could be thrust into the role of auditing each network's address usage with the implicit threat of taking away the resources if the allocation is no longer consistent with policy. As one RIPE-NCC document admitted, "Many resources are now used for other purposes than they were originally assigned for. Certifying such resources would seem to imply that the RIPE NCC has validated

terms and conditions regarding the revocation of the certificate. But more importantly, getting a certificate from an RIR greatly changes the power relationship between the ISP and the address allocation authority. The internet has evolved in a way that detaches responsibility for address allocation from operational responsibility for routing. The RIRs, which are membership organizations of ISPs, register and record address block assignments in order to keep them unique. While ISPs use the RIRs' address allocations database, Internet service providers wholly control and authorize what routes they announce, and decide for themselves which other ISPs' routing announcements they trust or filter. Indeed, the RIRs' authority over address usage is almost completely a byproduct of the ISPs' willingness to use their registries as coordination tools.

RPKI changes all that. It has the potential to give RIRs direct, operational impact on routing. IAB member Danny McPherson first called attention to the way RPKI might give an RIR control over what is routed – and therefore stronger influence over what information is accessible over the internet. Reinforcing this view, David Conrad, at that time the head of IANA, wrote on the SIDR list:

> "Today, RIR influence on routing is essentially advisory in nature -- if an address holder (say) fails to pay their address maintenance fee, RIRs can, at most, remove the address holder's blocks from Whois databases. However, as I understand it, this has limited effect on existing [routing arrangements]. The RIR could potentially reallocate the space, but this would likely be a good way of annoying multiple parties (not just the folks the address space was reclaimed from). …[I]f filter lists are built or routers check origin authenticity in real-time by traversing the RPKI tree(s), there would seem to be significantly more control vested in each parent node in the path up to the root of the RPKI hierarchy. My fear is that this will simply be unacceptable in a political or business sense." [7]

Confirming Conrad's point, a university network operator objected to the way RPKI altered "the balance of power" between network operators and the RIRs:

> "Today if there is a legal dispute between an allocator [RIR] and an organization with an allocation, it will be solved through existing civil means. This may take some time. In the meantime the status quo

this re-assignment." See RIPE document 070206, "Outline new and current services affected by certification." Draft v1.5 https://ripe59.ripe.net/ripe/maillists/archives/ca-tf/2007/doc00000.doc.

[7] David Conrad, post to SIDR WG list 17 September 2009. http://www.ietf.org/mail-archive/web/sidr/current/msg01098.html.

> continues (from a technical/operational perspective). With RPKI the allocator can revoke the organization's certificate while the civil process takes its time, causing harm to the organization that is now unroutable. Don't think they won't do the revocation. I have personally seen situations where if one party has 'the switch' to enforce their will, they use it." [8]

Predictably, revocation of certificates has emerged as a critical point of contention in the ISP community's debates over RPKI. For example, when RIPE-NCC proposed implementing resource certification, its members refused to support it due to concerns about the length of certificate validity and the linking of certificate revocation to RIPE membership status. Participants commented that "people will be reluctant to [use resource certificates] if they have reasons to fear that routing may be stopped due to unexpected events relating to certificates' revocation." [9] Clearly, RPKI diminishes the autonomy of ISPs. It could be used to replace a looser, networked form of governance based on decentralized associative choices among Internet service providers with a more centralized and hierarchical governance form.

***Trust model and global compatibility***

An RPKI relies on a hierarchical chain of trust. This raises an important question: what organization or institution serves as the root-level trust anchor for the certification hierarchy? If there is no such centralized root, how does one ensure global compatibility and trust? This is the problem that creates divergent incentives for the other three actors (the RIRs, ICANN and the U.S. Government).

In the classical PKI scenario, everyone trusts a single Certification Authority (CA) and the sender and recipient of the information rely on the same CA. This kind of centralization is relatively easy to achieve in a single organization. [10] It becomes harder and harder to achieve as the set of

---

[8] Jeff Schiller, MIT network operator, post to the SIDR WG email list, September 20, 2009. http://www.ietf.org/mail-archive/web/sidr/current/msg01117.html.

[9] See http://www.ripe.net/ripe/maillists/archives/ca-tf/2009/msg00013.html.

[10] "In the classical PKI scenario, someone receives a document signed with a digital certificate. The recipient must trust the creator of that certificate (the Certification Authority - CA) to be able to confirm the identity of the sender. This is simple if the sender and recipient are using the same CA. The need for interoperability arises where the document has been signed with a certificate from a CA that the recipient does not know. The obvious approach is to centralise as much trust as possible and avoid this problem entirely. This is reflected in the root CA and

organizations using it becomes larger and more diverse. Even the U.S. government could not agree on a single CA for all its PKI activities. The global internet, which involves approximately 35,000 autonomous systems and hundreds of thousands more sub-delegations of address resources across hundreds of different language groups and political systems, the goal of a centralized and unified trust anchor may be unrealistic – and potentially even disruptive and dangerous, as the political battles over the root of the domain name system (DNS) have already demonstrated (MUELLER, 2010, KUERBIS & MUELLER, 2007). Insofar as one uses a centralized, strictly hierarchical trust model, one is also creating the potential for centralizing political and regulatory authority over the Internet.

The SIDR working group – significantly influenced by researchers supported by U.S. military contracts – wanted to map the resource allocation hierarchy directly onto the PKI, to make it as technically simple and unambiguous as possible. However, its deliberations explicitly noted the political and governance issues associated with that. In an attempt to square the circle, SIDR's architectural specification allowed organizations to choose their own trust anchor. The RPKI standard codified its reliance on the IANA-RIR allocation hierarchy; at the same time, its design was described as "capable of accommodating a variety of trust anchor arrangements." (HUSTON, WEILER, MICHAELSON & KENT, 2010) A statement by the SIDR WG's co-chair summed up the policy in a colorful way – and also revealed how ambiguous the underlying attitudes and specifications were:

> "[…] the ability of a relying party to choose a trust anchor is a big get-out-of-jail-free card for those who are allergic to the idea of one root. NOT that I'm recommending using that card." [11]

While the ability of ISPs to choose their own trust anchor might lead to a more heterogeneous yet compatible certification system, it is also possible that once the system achieves a critical mass of adopters, network effects will lead to convergence on a single, centralized trust anchor. In that case, ISPs who do not use the same trust anchor will face compatibility problems that could literally break their routing arrangements, cutting off their users from global connectivity. That risk would force everyone to rely on the dominant certification hierarchy and its trust anchor. As long as it is unclear

hierarchy PKI models discussed below. However, those models require tight central control and unanimous support." (Galexia, 2005 p. 4).

11 Sandra Murphy in post to SIDR WG list, 1 December 2008. http://www.ietf.org/mail-archive/web/sidr/current/msg00733.html.

how RPKI achieves compatibility among multiple roots, it is disingenuous to pretend that RPKI allows ISPs a free choice of trust anchors – just as it is disingenuous to pretend that anyone who wants to create an alternate DNS root can easily do so.

***The incentives of the USG and ICANN***

The U.S. government (USG), through the IANA contract, controls the top level of the address allocation hierarchy. ICANN is the party that the USG has chosen to perform the IANA functions.[12] The same contract gives ICANN control of the root of the domain name system hierarchy as well as the address space. While the USG's control of the IANA functions does contribute to the implementation of an effectively globalized governance regime, it is also a persistent source of political controversy, in that it elevates one national government over others.[13] It may also create advantages for US military[14] and surveillance capabilities, as well as providing economic and technological advantages for specific U.S. businesses. The U.S. government has made it clear that it considers retaining unilateral control of the IANA contract a matter of high-level national interest.[15] It has also funded much of the research work on RPKI. The U.S. Department of Homeland Security's Internet Infrastructure Security (IIS) program, part of its National Strategy to Secure Cyberspace, made its support for RPKI explicit: as part of the IIS program, DHS expected to "develop and deploy a Public Key Infrastructure (PKI) with the American Registry for Internet Numbers (ARIN)" by 2008, and to "conclude PKI deployment activities with global registries" by 2010.[16] Researchers and organizations that are part of the U.S., or are contractual agents of the U.S.

---

12 The contract between the Department of Commerce and ICANN and its various revisions is available at http://www.ntia.doc.gov/ntiahome/domainname/iana.htm.

13 See DRAKE (2005); MAYER-SCHÖNBERGER & ZIEWITZ (2007); and MUELLER (2010) for a discussion of the role of U.S. unilateral control over IANA in sparking geopolitical controversy during and after the World Summit on the Information Society (2002-2005).

14 Some of the political implications were noted by IAB member D. McPherson, who wrote "If some country holding the keys (TA) goes to war with another and decides they want to revoke all of their allocations, then ISPs would have zero control over this outside of their own routing domain." Danny McPherson, post to SIDR WG list 11 March 2008, http://www.ietf.org/mail-archive/web/sidr/current/msg00346.html. The concern over "bringing down national network infrastructures" and the relationship to a single authoritative trust anchor residing with IANA (which maintains a contractual relationship with a single government) were expressed again in a recent European study (ENISA 2010b).

15 See http://www.ntia.doc.gov/ntiahome/domainname/usdnsprinciples_06302005.htm.

16 See http://www.dhs.gov/xlibrary/assets/SandT5yearplan.pdf, pp. 3 and 53.

such as ICANN, support a RPKI hierarchy completely tied to the address allocation hierarchy, with IANA as the single root at the top of the hierarchy. The U.S. has an incentive to bring about a single-root hierarchy because it maintains and reinforces its own control over critical internet resources.

The organizational ambitions of ICANN also point in the direction of a single-root RPKI hierarchy with the IANA at its apex. Currently, ICANN plays a diminished role in address allocation. Until now the linkage between IP address governance and ICANN's governance of the domain name system has been fairly loose. The three major RIRs (RIPE, ARIN and APNIC) actually predate ICANN, and obtained most of the address resources they administer prior to the creation of ICANN in 1998. ICANN's Address Supporting Organization has never been formally established as an independent entity and the RIRs' trade association, the Number Resource Organization, has never signed a formal contract with ICANN that binds the NRO to ICANN's rules or contracts. Instead, the RIRs and ICANN are joined through a loose and noncommittal memorandum of understanding. Indeed, whereas ICANN gets over $50 million a year in fees from its contracts with domain name registries and registrars, it collects less than a million in "voluntary contributions" from the RIRs. Whatever fees they do pay are set by their own decisions and processes, not ICANN's. The relatively autonomous position of the RIRs emerged accidentally, as an artifact of the Internet's unplanned emergence in the mid-1990s. From the standpoint of the decentralization of power over Internet governance, these informal relationships are a good thing in certain respects. But RPKI threatens to reconfigure them.

There is some fear on the part of the USG-aligned interests that the NRO has ambitions to take control of the address space away from IANA/ICANN. If this happened it would diminish ICANN's stature and potential for revenue. Thus it is not surprising that we see ICANN eagerly embracing RPKI and pushing for a more centralized trust anchor located in the IANA. In its most recent Plan for Enhancing Internet Security, Stability & Resiliency ICANN's staff wrote that "ICANN, through management of the IANA functions, acquires the strategy and the responsibility of the stability, security and resiliency of the Internet number allocation system and ultimately, through the application of Resource Public Key Infrastructure (RPKI), the global Internet routing system. This responsibility manifests in the need to implement a technically ideal application of the RPKI Single Trust Anchor, as noted by the IAB and NRO, and results in ability to fully certify the validity, right of use, and uniqueness of Internet number resources." (ICANN 2010) In June 2008, ICANN's Security and Stability Advisory Committee (SSAC)

indicated its interest in "management of certificates for the addressing system (RPKI)." Indicating the alignment of interests between ICANN and the U.S. government, the U.S. Department of Homeland Security's IIS program manager was added to ICANN's Security and Stability Advisory Committee, and ICANN's 2010-11 fiscal budget included financial support for managing RPKI certificates.

***The incentives of the RIRs***

RPKI puts the RIRs in the center of many internet governance issues by dramatically expanding their authority over the day to day use of Internet number resources. It also heightens the tensions surrounding their relationship to ICANN/IANA.

The RIRs favor linking certificates to the address allocation hierarchy but they are also uncomfortable with a RPKI scheme that has a single trust anchor located at the IANA. Their preferred solution is to have six co-equal roots, one operated by the IANA and the other five by each of the five RIRs.

The RIRs' understand that reliance on a single trust anchor operated by the IANA has the potential to radically change their relatively autonomous position, by empowering ICANN/IANA to exert more direct control over the issuance and revocation of their address resources. This could lead them inexorably into a more formal contractual relationship with ICANN, more formalized fee-paying obligations, and a more direct subordination of their policy processes to ICANN's. Moreover, there is some hope in the technical community that when the current IANA contract expires, the U.S. government will alter the IANA contract in a way that will bring an end to ICANN's sole possession of it. Thus, despite the support expressed by the NRO and the IAB for a single trust anchor for RPKI, neither explicitly proposes to make ICANN the root. This was evident from a statement they issued in 2009, which said:

> "The Regional Internet Registries (RIRs) believe that the optimal eventual RPKI configuration involves a single authoritative trust anchor. That configuration may not be achievable in the short-term and the details and timelines for its implementation will depend among other things on discussions within the RIRs' communities and dialogues with others including the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF). In the meantime, the RIRs have agreed to undertake pragmatic implementations of RPKI services based on interim trust anchor models..." (NRO, 2009)

If ICANN was the exclusive root trust anchor for the RPKI, it might be possible for it to disintermediate the RIRs, and issue certificates and address blocks directly to organizations and end users.

Aside from the IANA/ICANN issue, the RIRs have strong organizational incentives to favor implementation of RPKI. It would strengthen enormously their role in Internet operations, creating opportunities to put more "teeth" or enforcement power into their policies. It would make revocation of address resources self-enforcing; it could also be used to rigidly enforce the territorial exclusivity of each RIR's address pools.

If RPKI became so widely adopted that most ISPs refused to route packets from entities not participating in the RPKI, such a requirement would make membership in the RIRs virtually compulsory and their fees a kind of tax rather than a membership payment for a voluntarily selected set of services and organizational rights. One ISP expressed fears about the monopoly power of the RIRs during the SIDR working group:

Although there is plenty of sense in aligning the RPKI chain of trust with the resource allocation chain, ISPs may have concerns with the RIRs being the trust anchors. The incentive structure for the RIRs is fundamentally different than that of a [private market] certificate provider like Verisign/Thawte/ CyberTrust. If these root CAs time and again demonstrate that they are untrustworthy they lose customers, revenue, and potentially their trusted status. What entices an RIR toward vigilance as they validate the supposedly authorized origin of a prefix? [17]

## ■ Concluding observations

This paper has documented contention over the adoption of a security technology, RPKI. The contention is caused by the way the technology's implementation bases routing security on resource certificates issued by the institutions that issue IP addresses.

As the first facet of its analysis, the paper analysed the shifts in power and cost-benefit distributions that arise from RPKI's implementation. It

[17] Ryan Shea, Senior Engineer, Network and Info Security, Verizon Business in post to SIDR WG email list 22 September 2009.
http://www.ietf.org/mail-archive/web/sidr/current/msg01142.html.

demonstrated that in this area, as in so many other areas of security technology requiring coordinated action among multiple stakeholders, there is no simple progression from a less secure to a more secure state, with the improvements in security being homogenous across all actors. On the contrary, the effort to achieve collective security via RPKI alters the distribution of power and economic benefits among different types of actors. For ISPs especially, RPKI creates a major new dependency with very important economic and regulatory implications. Issuers of the certificates could literally shut off an ISP's routing operations. This would potentially give address allocation authorities (or governments issuing orders to them) direct operational effects on ISPs.

As the second facet of the analysis, the paper asked how the incentives created by these prospective redistributions of power and wealth affect the possibility that the technology will be adopted. A key fact is that the IP address allocation mechanisms to which RPKI certificates would be tied are strictly hierarchical. Predictably, given the economic and political dependencies created by a hierarchical PKI, the four key categories of stakeholders (ISPs, RIRs, ICANN and the U.S. government) have taken positions on the implementation of RPKI based on their position within the hierarchy. The two parties at the top of the address allocation hierarchy (ICANN, U.S.) are enthusiastic supporters of RPKI implementation with a single, unified trust anchor. Those in the middle of the hierarchy (the RIRs) support RPKI implementation but seek a slightly less centralized trust anchor. Such a regime would maintain their financial and policy autonomy from ICANN while allowing them to run their own certification authorities. Actors at the bottom of the hierarchy (the ISPs) are unenthusiastic about rigidly linking routing to the address allocation hierarchy and for the time being show little inclination to adopt RPKI en masse. They are deeply concerned about the potential loss of autonomy inherent in such an approach.

These varying incentives have interesting, complex impacts on adoption. The conflict over positioning within the hierarchy has given the RIRs a strong incentive to implement RPKI rapidly using multiple trust anchors rooted in their own organizations. The RIRs have implemented RPKI as a voluntary member service as a pre-emptive move. ICANN and the U.S. government are not ready to roll out a globalized RPKI implementation that they could impose upon the RIRs yet. By acting now, and achieving some usage, the RIRs make it more difficult for ICANN to later bypass them.

Note that the barriers to ISP adoption do not come from network externalities *per se*. While it is true that the security benefits are not fully realized until most other ISPs adopt compatible RPKI, pairwise combinations of ISPs can achieve small increases in routing security incrementally. The real sticking point for ISPs is the loss of autonomy vis-a-vis their address registry. Network externalities could play a major role in the story, however, if any single trust anchor achieves critical mass and begins to establish itself as the dominant hierarchy.

For the time being, the conflict over position in the hierarchy has been resolved by permitting significant scope for voluntary action by each actor. For better or worse, the Internet remains a space where authority is highly distributed and no one is in a position to tell the others what to do. But elements of hierarchy do exist, especially around critical resource allocation, and it is likely that security and other concerns will lead to continuing efforts to leverage those hierarchies into more powerful governance arrangements.

**References**

ANDERSON, R. & MOORE, T. (2006): "The Economics of Information Security", *Science*, 314(5799), 610-613.

BARBIR, A., MURPHY, S. & YANG, Y. (2006): *Generic Threats to Routing Protocols, RFC 4593*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc4593.

BAUER, J.M. & VAN EETEN, M.J.G. (2009): "Cybersecurity: Stakeholder incentives, externalities, and policy options", *Telecommunications Policy*, 33(10-11), 706-719.

BUTLER, K., FARLEY, T., McDANIEL, P. & REXFORD, J. (2010): "A Survey of BGP Security Issues and Solutions", *Proceedings of the IEEE*, 98(1), 100-122. doi: 10.1109/JPROC.2009.2034031.

BUSH, R., AUSTEIN, R. & BELLOVIN, S. (2010): "The RPKI & Origin Validation". http://www.ripe.net/ripe/meetings/ripe.../Bush-The_RPKI_Origin_Validation.pdf.

DRAKE, W. (Ed.) (2005): "Reforming Internet Governance: Perspectives from the UN Working Group on Internet Governance", New York: United Nations Information and Communication Technologies Task Force.

ECONOMIDES, N.:

- (1996): "The economics of networks", *International Journal of Industrial Organization*, 14(6), 673-699.
- (1994): "Networks and compatibility: Implications for antitrust", *European Economic Review*, 38(3-4), 651-662.

European Network and Information Security Agency [ENISA] (2010): Report on secure routing technologies. http://www.enisa.europa.eu/act/res/technologies/tech/routing/report-on-secure-routing-technologies/at_download/fullReport.

Galexia (2005): *PKI Interoperability Models*. http://www.galexia.com/public/research/assets/pki_interoperability_models_2005/pki_interoperability_models_2005.pdf.

HU, Y., McGREW, D., PERRIG, A., WEIS, B. & WENDLANDT, D. (2006): "(R)Evolutionary Bootstrapping of a Global PKI for Secure BGP", In *Workshop on Hot Topics in Networks (HotNets'06)*, Irvine, CA. http://sparrow.ece.cmu.edu/group/pub/hu_mcgrew_perrig_weis_wendlandt_bgp.pdf.

HUSTON, G., WEILER, S., MICHAELSON, G. & KENT S. (2010): *Resource Certificate (RPKI) Trust Anchor Locator*, Internet Engineering Task Force. http://tools.ietf.org/html/draft-ietf-sidr-ta-06.

Internet Corporation for Assigned Names and Numbers [ICANN] (2010): *Plan for Enhancing Internet Security, Stability & Resiliency*. http://www.icann.org/en/topics/ssr/ssr-draft-plan-fy11-13sep10-en.pdf.

Internet Architecture Board [IAB] (2010): *IAB statement on the RPKI*. http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html.

KENT, S. (2006): "An Infrastructure Supporting Secure Internet Routing", in A.S. ATZENI & A. LIOY, *Public key infrastructure: Third European PKI Workshop: Theory and Practice*, Lecture Notes in *Computer Science* (Vol. 4043, pp. 116-129). Berlin, Heidelberg: Springer Berlin Heidelberg.

KUERBIS, B. & MUELLER, M.L. (2007): "Securing The Root: A Proposal For Distributing Signing Authority. Internet Governance Project". http://internetgovernance.org/pdf/SecuringTheRoot.pdf.

LELARGE, M. (2009): "Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives", *The Eighth Workshop on the Economics of Information Security*, University College, London.

MAYER-SCHÖNBERGER, V. & ZIEWITZ, M. (2007): "Jefferson Rebuffed - The United States and the Future of Internet Governance", *The Columbia Science and Technology Law Review* 8, no. 188.

MUELLER, M.L.:

- (2010): *Networks and States: The global politics of Internet governance*, MIT Press.
- (1997): *Universal Service: Competition, Interconnection and Monopoly in the Making of the American Telephone System*, MIT Press.

Number Resource Organization [NRO] (2009): *NRO Statement on RPKI*. http://www.nro.net/news/nro-declaration-rpki.html.

REHKTER, Y., LI, T. & HARES, S. (2006): *A Border Gateway Protocol 4 (BGP-4)*. *RFC 4271*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc4271.

REKHTER, Y. & LI, T. (1995): *A Border Gateway Protocol 4 (BGP-4)*. *RFC 1771*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc1771.