The ISP Column
A monthly column on things Internet

December 2008

Geoff Huston

Resource Certification

In November 2008 APNIC publically released its resource certification toolkit. This system allows a holder of APNIC-allocated IP number resources (IP addresses and AS numbers) to have these resources certified by APNIC as being currently held by the entity through the issuance and publication of a digital resource certificate. The system also allows every such resource holder to generate signed attestations and digital authorities relating to the use of their allocated address space in a routing context, or within other administrative or technically focussed processes that can make use of verifiable attestations relating to a holder's current "right-of-use" over such IP number resources. In this article I will look at resource certificates in some detail, looking at the technology that underpins certification structures, and the potential use of these instruments in securing inter-domain routing and potentially in the area of the emerging need to support address transfers in IPv4.

Opinions vary as to what aspect of the Internet's infrastructure represents the greatest common vulnerability to the security and safety of Internet users, but it is generally regarded that attacks that are directed at the network's infrastructure are the most insidious, and in that case the choice is probably between the Domain Name System (DNS) and the inter-domain routing system.

The question of how to improve the robustness of these functions has been a longstanding topic of study. For the DNS it appears that there is convergence on DNSSEC as the technical solution to securing DNS resolution operations, and the focus of attention in this space has shifted from technical behaviour to issues relating to operational deployment. It has been a long haul for DNSSEC and to say that there is an end in sight may well be premature at this stage, but there are definite signs of progress in this space. The same cannot be said of progress with securing routing, and particularly in securing inter-domain routing. Here there is still much to be done in order to achieve reasonable consensus on what technical measures to adopt, let alone the second step of study of how such measures could be deployed across the Internet.

The IETF's approach to addressing the topic of securing inter-domain routing has followed a conventional IETF path. The first step has been to consider the nature of various vulnerabilities that exist within today's inter-domain routing system and then develop a set of requirements that should be addressed in any solution space, without necessarily defining what such a solution may be. Once the enumeration of requirements achieve a suitable level of consensus

from the community it is then possible to commence work on standardizing solutions. In the case of securing inter-domain routing the first steps were undertaken in BOF sessions and in the subsequently formed Routing Protocol Security Requirements (RPSEC) Working Group. This work is almost complete, and apart from some definitive statement relating to a requirement for securing the AS Path attribute in BGP, the set of requirements for securing inter-domain routing is now in a close to final state. The task of the Securing Inter-Domain Routing (SIDR) working group is to standardize technologies that can meet these requirements.

So where does "Resource Certification" come into the picture?

Public Key Cryptography

One commonly used security technology is public key cryptography, As long as a suitable amount of vague hand waving is used, the technique can be easily explained. The approach uses a pair of keys, A and B. Anything enciphered with key A can only be deciphered with Key B, and vice versa, and knowledge of the value of one key does not lead to discovery of the value of the other key. Key A is kept as a closely guarded secret, while key B is openly published. If I want to send you a message that only you can decipher and read I should encrypt it using your public key. If I want to send you a message that only I could've sent (non-repudiation) then I'll generate a digital signature of the message using my private key, That way any attempts to alter the message will also be detectable.

This latter approach, of using keys to generate digital signatures of messages, lies at the heart of DNSSEC, as DNSSEC adds public keys and digital signatures to the DNS. A DNS query can generate a response that lists both the DNS answer and the digital signature of that answer. The DNS can also be queried to retrieve the public key used to sign all the components of that zone, so that the digital signature can be verified and the query agent can be assured that the response is a genuine one. But how can the key itself be verified? IN DNSSEC the hierarchical nature of the DNS itself is exploited by having each zone 'parent' sign the keys of its delegated 'children'. So the zone key can be verified by retrieving the parent's signature across that zone key, and so on to the root of the DNS. As long as the query agent knows beforehand the value of the public key used to sign the root zone of the DNS, and as long as DNSSEC is used universally, all DNS responses can be verified in DNSSEC.

While this approach works in the interlocked hierarchical structure of the DNS, when we turn out attention to securing the use of IP addresses and AS numbers in the context of inter-domain routing, then there is no comparable hierarchy to exploit. In such cases a common solution is to turn to Digital Certificates.

Digital Certificates are a digitally signed public attestation by a certification authority that associate a subject's public key value with some attribute of the subject. A very typical application is in identity certification, where the certification authority is attestation that the holder of the private key whose matching public key is provided in the certificate has met the authority's certification criteria to be identified by a particular name. Digital certificates are useful in that they are able to reduce the number of trust points in a security domain, so that each member of the domain does not have to validate identity and exchange public keys with every other member of the domain, but can undertake a single transaction with a certification authority that is trusted by all the members of the domain. As long as every member of the domain carries the public key of the certification authority and can access all issued digital certificates, then the members of the domain can verify each other's attestations and digital signatures.

Of course digital certificates are used for far more than attestations of identity, and can encompass the authority to perform specific tasks, undertake particular roles, or grant permissions and right-of-use authorities. It is this latter use case that is relevant to resource certification.

Resource Certificates

A resource certificate is a conventional X.509 certificate that conforms to the PKIX profile with one critical component, namely a certificate extension that lists a collection of IP number resources (IPv4 addresses, IPv6 addresses and AS Numbers).

These certificates attest that the certificate's issuer has granted to the entity represented by the certificate's subject a unique "right-of-use" of the associated set of IP number resources listed in the certificate's extension, by virtue of an associated resource allocation. The unique "right-of-use" concept mirrors the resource allocation framework, where the certificate provides a means of third-party validation of assertions related to resource allocations.

By coupling the issuance of a certificate by a parent Certification Authority (CA) to the corresponding resource allocation, a test of a certificate's validity including the IP number resource extension can also be interpreted as validation of that resource allocation. Signing operations which descend from that certificate can therefore be held to be testable, under the corresponding hierarchy of allocation. In other words, if you received your address block from a particular RIR, then only that RIR can issue a resource certificate for you that includes your public key and the allocated number resources. Anything you sign using your private key can be verified via the RIR's issued certificate.

Unlike certificates that relate to attestations of identity, resource certificates are not necessarily long-lived. When an additional allocation action occurs, the associated resource certificate is reissued with a IP number resource extension that matches the new allocation state. In the case of a reduction in allocated resources the previously issued certificates are explicitly revoked once the new certificate is issued. In other cases there is no explicit revocation of the older certificates.

The intention here is that any instrument signed by the subject's private key that relates to an assertion of resource control, whether it's a protocol message in a routing protocol or an administrative request to an ISP to route a prefix or as assertion of title over the "right-of-use" of a number resource, can be validated through the matching public key contained in the certificate and the IP number resource that are enumerated in this certificate. The resource certificate itself can be verified in the context of a resource certificate Public Key Infrastructure.

The Resource Certificate Public Key Infrastructure

The Resource Certificate Public Key Infrastructure (RPKI) describes the structure of the certification framework used by Resource Certificates. The intent of the Resource Public Key Infrastructure (RPKI) is to construct a robust hierarchy of X.509 certificates that allows relying parties to validate assertions about IP addresses and AS Numbers, and their use.

The structure of the RPKI as it relates to public use of IP number resources is designed to precisely mirror the structure of the distribution of addresses and AS's in the Internet, so a brief description of this distribution structure is appropriate. The Internet Assigned Number Authority (IANA) manages the central pool of number resources. The IANA publishes a registry of all current allocations. The IANA does not make direct allocations of number resources to end users or Local Internet Registries(LIRs), and, instead allocates blocks of number resources to the Regional Internet Registries (RIRs). The RIRs perform the next level of distribution, allocating number resources to LIRs, National internet Registries (NIRs) and end users. NIRs perform allocations to LIRs and end users, and LIRs allocate resources to end users. (Figure 1)

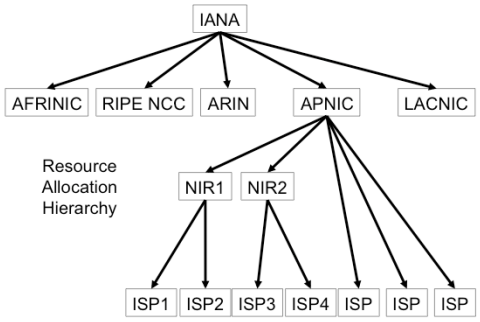

Figure 1. Address Distribution Hierarchy for the Internet

The RPKI mirrors this allocation hierarchy. One interpretation of this model would see the IANA manager a root RPKI key and using this key the IANA would issue a self-signed "root" certificate, and also issue subordinate certificates to each of the RIRs, describing in the resource extension to the certificate the complete set of number resources that have been allocated to that RIR at the time of issuance. The certificate would also hold the public key of the RIR and would be signed by the private key of the IANA. Each RIR would issue certificates that correspond to allocations made by that RIR, where the resource extension to those certificates lists all the allocated resources, and the certificate includes the public key of the recipient of the resource allocation, signed with the private key of the RIR. If the recipient of the resource allocation is an LIR or an NIR then it too would also issue resources certificates in a similar vein (Figure 2).

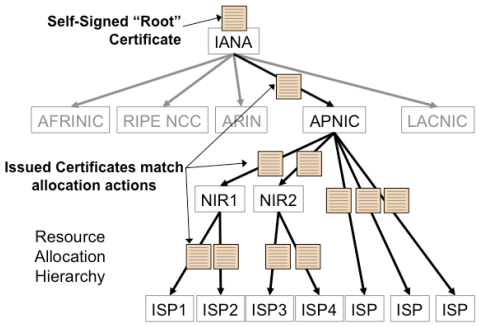

Figure 2. RPKI Resource Certificate Hierarchy

The common constraint within this certificate structure is that an issued certificate must contain a resource extension that contains a subset of the resources that are described in the resource extension of the issuing authority's certificate. This corresponds to the allocation constraint than a registry cannot allocate resources that were not allocated to the registry in the first place. One implication of this constraint is that if any party holds resources allocated from two or more registries then it will hold two or more resource certificates in order to describe the complete set of its resource holdings.

Validation of a certificate within this RPKI is similar to conventional certificate validation within any PKI, namely establishing a chain of valid certificates that are linked by issuer and subject from a nominated trust anchor CA to the certificate in question. The only additional constraint in the RPKI is that every certificate in this validation path must be valid resource certificates, and that the IP number resources described in each certificate are a subset of the resources described in the issuing authority's certificate.

Within this RPKI all Resource Certificates must have the IP Addresses and AS Resources present, and marked as a critical extension. The contents of these extensions correspond exactly to the current state of IP address and AS number allocations from the issuer to the subject.

Any holder of a resource who is in a position to make further allocations of resources to other parties must be in a position to issue Resource Certificates that correspond to these allocations. Similarly, any holder who wishes to use the RPKI to digitally sign an attestation needs to be able to issue an End Entity (EE) certificate to perform the digital signing operation. For this reason all issued certificates that correspond to allocations are certificates with the Certification Authority (CA) capability enabled, and each CA certificate is capable of issuing subordinate CA certificates that correspond to further sub-allocations and subordinate EE certificates that correspond to generation of digital signatures on attestations.

The RPKI makes conventional use of Certificate Revocation Lists (CRLs) to control the validity of issued certificates, and every CA certificate in the RPKI must issue a CRL according to the CA's nominated CRL update cycle. A CA certificate may be revoked by an issuing authority for a number of reasons, including key rollover, the reduction in the resource set associated with the certificate's subject, or termination of the resource allocation. To invalidate the authority or attestation that was signed by a given EE certificate, the CA issuing authority that issued the EE certificate simply revokes the EE certificate.

Resource Certificates are intended to be public documents, and all certificates and objects in the RPKI are published in openly accessible repositories. The set of all such repositories forms a complete information space, and it is fundamental to the model of securing the public Internet's inter-domain routing system that the entire RPKI information space is available. Other uses of the RPKI might permit use of subsets, such as the single chain from a given end-entity certificate to a Trust Anchor, but routing security is considered against all known publicly routable addresses and AS numbers, and so all known resource certification outcomes must be available. In other words the RPKI's intended use in routing contexts is not a case where each relying party may make specific requests for RPKI objects in order to validate a single object, but one where each relying party will perform a regular sweep across the entire set of RPKI objects in order to ensure that the relying party has a complete picture of the RPKI information space. This aspect of the RPKI represents some interesting challenges, in that rather that having a single CA publish all the certificates produced in a security application at a single point, the RPKI permits the use of many publication points in a widely distributed fashion. Each CA is able to issue RPKI objects and publish them using a locally managed publication point. It is incumbent upon relying parties to synchronise a locally managed cache of the entire RPKI information space at regular and relatively frequent intervals. For this reason the RPKI has introduced an additional mechanism in its publication framework, namely the use of a "manifest" to allow relying parties to determine whether they have been able to retrieve the entire set of RPKI published objects from each RPKI repository publication point, or if there has been some attempt to disrupt the relying party's access to the entire RPKI information set. It also implies that the RPKI publication point access protocols should support the efficient function of a synchronization comparison, so that a locally managed cache of the RPKI need only call for the uploading of those objects that have been altered since the previous synchronization operation.

Signed Attestations and Authorities

The underlying intent of digital certificates, and resource certificates in particular, is in terms of supporting a transitive trust relationship that allows a relying party to verify the authenticity of a signed artefact through verification of the signer's key using the PKI. So the obvious question is what artefacts are useful to sign?

Much of the motivation for resource certificates has come from a desire to underpin efforts in securing aspects of inter-domain routing. This goes well beyond securing the individual point-to-point connection used between BGP speakers, and refers to the issue of verifying the authenticity of the payload of the BGP protocol exchange. The specific question that may be posed is: how can a BGP speaker validate the authenticity of the route object being presented to it?

The approach being studied by the SIDR WG is to use structured attestations, where, like the digital certificate itself, the attestation is structured in an ASN.1 digital object, and this object is signed using a signing formation which is itself a piece of structured ASN.1, namely the Cryptographic Message Syntax (CMS) [RFC3852].

The first of these attestations relates to the ability to verify the authenticity of the "origination" of an inter-domain routing object. This refers to the address prefix and the originating AS, and the questions that this verification function is intended to answer are:

- Is this a valid address prefix and AS number? Have these resources been allocated through the IP number resource allocation process?
- Has the holder of the title of "right-of-use" for the address prefix authorized the AS holder to originate a routing advertisement for this prefix?

Here an address holder is authorizing a particular ISP to generate a route announcement for their particular address prefix. In this case the prefix holder would generate an EE resource certificate with the IP number resource extension spanning the set of addresses that match the address prefixes that are the intended subject of the routing authority, and place validity dates in the EE certificate that correspond to the intended validity dates of the routing authority. The signed authority document would contain the Autonomous System number that is being authorized in this manner, and a description of the range of prefixes that the prefix holder has authorized, and the EE certificate. The document would be signed by the EE certificate's private key using a CMS signing structure. The resultant object is published in the RPKI distributed publication repository as a Routing Origination Authorization (ROA). A relying party can validate the ROA by checking that the digital signature in the ROA is correct, indicating that the authority document has not been tampered with in any ay since it was signed, that the resources in the associated EE certificate encompass the prefixes specified in the document, and the EE certificate itself is valid in the context of the RPKI by verifying that there is an issuer/subject chain of valid certificates that link one of the relying party's nominated Trust Anchors to the EE certificate.

The ROA itself is valid as long as the signing EE certificate is valid. To withdraw the authority prior to the expiration of the EE certificate the ROA publisher can simply revoke the EE certificate. This leads to the concept of "one-off-use" EE certificates in the RPKI, where an key pair and a corresponding EE certificate is generated in order to sign a single attestation or authority. If he authority's lifetime is extended, the authority is re-issued with a new EE certificate, and with a new digital signature, and, as noted, the authority can be prematurely terminated through revocation of the EE certificate, so at no stage is there a need to reuse the original signing private key. Once the private key is used to sign this object, the key is destroyed, alleviating to some extent the load key management load.

In any security system knowledge of what is authorized is helpful, but knowledge of what has not been authorized is perhaps even more helpful. For ROAs there is an analogous situation to DNSSEC, where DNSSEC is most effective from a client's perspective once the entire DNS space is DNSSEC signed. Where there are gaps in the DNSSEC signing chains the client is left in an uncertain state regarding the verification outcomes of the unlinked DNS sub-hierarchies. The same could apply to ROAs, in that in an environment where not every originated route object has a published ROA, then the absence of a ROA does not necessarily indicate an unauthorized route origination. If one of the objectives of this study is to define a framework that can unambiguously identify the unauthorized use of IP number resources in routing (route "hijacks") even in a world where ROAs are used in a piecemeal fashion, then one possible refinement to the ROA model is the introduction of a comparable negative authority, the Bogon Origination Attestation (BOA).

In this case the prefix holder generates a signed attestation, or BOA, in a similar manner to the ROA, but does not provide any originating AS. Instead the BOA refers to "all originating ASs", and has the semantic interpretation that any use in the routing space of this address prefix described in the BOA, or any more specific address prefix, should be regarded as unauthorized and the route should be discarded.

While this makes the detection of route hijacks more direct in a world of piecemeal use of ROAs there is now the added complication of having both "positive" and "negative" authorities. The proposed resolution of this is to use a relative priority rule that ROAs take precedence over BOAs, so that if a valid ROA and a valid BOA both exist that describes the origination component of a route, then the route can be regarded as authorized.

It should be noted, however, that at this stage these concepts "work in progress", and are part of the SIDR WG's agenda of study, and the WG has not as yet reached any consensus position regarding the decision to advance these proposals onward along the Internet Standards Process.

Also on the near term horizon for SIDR is examining approaches to secure the AS Path in BGP updates. The RPSEC WG has explored two approaches in this space. One involves an incremental multiple signature technique that allows a receiver of a BGP update to verify that the AS path described in the update is matched by a sequence of interlocking AS digital signatures using the RPKI. At the same time as an AS adds its own AS to the AS path prior to further eBGP propagation of the route update, the AS would digitally sign over an analogous sequence of AS signatures. This approach allows a received to perform a match of the AS sequence in the AS Path with the AS number sequence identified in the AS signature block. A match here would indicate that the BGP update has indeed been sequentially passed along the sequence identified by the AS Path. This approach was originally proposed in the secure BGP (sBGP) design and has attracted some comment related to the computation overhead associated with the application and validation of these AS Path signature sequences. An alternative approach has been one that is described by RPSEC as being less rigorous, and refers to a "feasibility" check, that checks that each pair of AS's represented in the AS Path has an associated verifiable assertion of inter-AS adjacency that is digitally signed by both AS's.

It should also be noted that this activity of addressing aspects of improving the robustness of inter-domain routing has some previous context. In many parts of the Internet some degree of routing integrity is managed through the use of Internet Routing Registries (IRRs) and the publication of routing policies through the use of Routing Policy Specification Language (RPSL) objects. While opinions vary as to the robustness of the security offered by the IRR approach, at the very least it can mitigate some weakness in the routing system through the use of a "second check" that can be used to filter the information that is being provided in a BGP feed. The weaknesses in the IRR system tend to relate to the consistency, completeness and authenticity of the IRR data, and in many cases the trust in the integrity of the data relies on the admission practices of the IRR itself and individual data objects cannot be verified by clients of the IRR. One possible way to address this has been through the use of Routing Policy System Security (RPSS) measures, but the adoption of these measures has not been widespread, and the question still remains for the client that even if an IRR object was authenticated upon admission, it does not mean that when the object is subsequently used by an IRR client the information reflects the current situation, and the information could well be invalid or not reflect the current policies of the IRR object's author.

One possible approach, being considered by the SIDR WG, is to implement the RPSS authentication models using object signing in the context of the RPKI. For example, the RPSS assumption that routes should only be announced with the consent of the holder of the origin AS number of the announcement and with the consent of the holder of the address space implies in RPSS that both parties should authorize the entry of a route object into the IRR. Translating this into an analogous model using the RPKI it would require that a route object be signed with the digital signatures of both the AS holder and the address space holder, and a IRR client can verify this route object at the time of use by verifying both digital signatures. Either the address space holder or the AS holder can revoke their authorization by revoking the EE certificate used to sign the route object, and the verification is independent of the particular IRR that has published the route object. Its also a possibility that the IRR itself can be folded into the RPKI distributed publication repository framework, as there is no particular requirement in such an environment for a disparate collection of IRRs with their own partial

collections of routing policy information, although at this stage this is heading into the realm of more advanced speculation about the potential for application of Resource Certificates and digital signatures to RPSL and the IRR framework.

Putting Resource Certificates into Context

Resource Certificates and the associated RPKI represent a major part of any effort to construct a secure inter-domain routing framework. An RPKI, even partially populated with signed information, allows BGP speakers to make preferential selections to use routing information where the IP address block and the AS numbers being used are recognised as valid to use, and that the parties using these IP addresses and AS numbers are properly authorized to so do. The RPKI can also be used to identify instances of unauthorised use of IP addresses and attempts to hijack routes.

However, the RPKI represents only one part of a larger framework of securing inter-domain routing, and the next step is that of applying the RPKI to the local BGP processing framework. There is also the need to move beyond validation of route origination and look at the associated issue of validation of the AS Path, and potentially to consider the most challenging task, of attempting to validate whether the initial forwarding decision associated with a route object actually represents the correct first hop along a useable forwarding path for packets to reach the network destination.

The issues here include not only a consideration of what can be secured and validated, but issues of scalability and efficiency in terms of deployment cost. The various approaches to routing security studied so far offer a wide variety of outcomes in terms of the amount of routing information that is validated, the level of trust that can be placed in a validation outcome and the overheads of generating and validating digital signatures on routing information. The next step appears to include the task of establishing an appropriate balance between the overheads of operating the security framework and the extent to which efforts to disrupt the routing system can be successfully deflected by such measures.

Resource Certificates and Transfers

Of course many readers may look at this with a wry smile and wonder at how long this will take to deploy.

Securing inter-domain routing is a longstanding topic, and progress in this area has been glacial at best. Even a minimal backward compatible change from 16-bit to 32-bit AS numbers has been problematical, and that was a change that was driven by the imperative of AS number pool exhaustion. Even more depressingly, the only aspect of the AS number change that excited any form of recent public comment was the somewhat bizarre topic of the appropriate representation to use for integers! If spending time worrying about numeric representational formats and disregarding all the more critical aspects of change in the inter-domain routing environment is the best that we can do here then its challenging to see how we can make any substantial progress in routing security, and tough to see why there is any imperative to proceed with resource certificates now, rather than awaiting the onset of the next geological era.

However, in the same fashion that the AS number pool is running out, I'm sure that most readers will be aware that as of December 2008 its abundantly clear the IPv4 unallocated address pool is going to run dry in the near future, or, if you've taken a couple of years to get to read this article then they have already run out!

However, unlike AS number exhaustion and 32-bit AS numbers, there is no elegant backward compatible solution here. If you are a IPv4-only system then the only way we can communicate is using an IPv4 packet, and that means I need to have some form of IPv4

address that I can present to you as my address in this communication. Whether I have to run my system in dual stack mode, or rely on a NAT-PT intermediary or a similar variant, I'll still need IPv4 and IPv4 addresses in some form or fashion.

So it seems that address transfers, and the related aspects of trading in IPv4 addresses, will be part of the environment in the coming years. But addresses are, from one perspective, just integers. And trading in integers does seem at first blush to be highly fanciful. While I've been personally somewhat attached to the number 3,406,445,568 for some time now, I find to hard to understand why I should want to "buy" this integer! Or even what value I should attach to this particular integer. What overloads these integers with value here is their interpretation in the context of IP networks, and while an attraction for 3,406,445,568 might seem to be a somewhat odd fetish, my attachment with the address prefix 203.10.60.0/24 is quite real and quite valuable for me right now.

What if I wanted to use this trading framework to acquire more addresses? How can I tell that the party representing themselves to me as a seller really has clear title to the addresses being proposed to be traded in this manner. And if we complete the transaction how can I be assured that I have clear and unique title to the "right-of-use" associated with these addresses, and that the other party's rights have been completely transferred to me? Its in this context that resource certificates may be useful.

In order to demonstrate that a party has a clear title to the "right-of-use" of an address prefix than the party should be able to generate a digitally signed attestation to that effect. The other party to such a transaction should be able to independently verify that attestation, again using the RPKI. While that allows some level of increased assurance as to the validity of the proposed address transfer transaction, the transaction itself need to be protected.

What are the desirable properties of a transfer function?

It would appear that it would require the explicit permissions of the resource disposer, the resource acquirer and the common resource issuer, or registry, in order to commence. In order to ensure the integrity of the transaction it may also require the resource registry to undertake some visible mutual exclusion lock that commits the resource disposer into this transaction with the resource acquirer to the exclusion of all other potential acquirers, for the period of the transaction. It may also need to place a time limit on the completion of the transfer transaction, at the expiration of which time if the transfer is not completed then the lock is removed and the incomplete transfer operation is annulled.

How could this be implemented?

One preliminary sketch of the way in which this might be supported is for the resource registry to operate the machinery of a transfer function. If resource transfers are permitted for resources issued by this registry, according to the registry's policy, then:

- A transfer would require both entities to be 'known' to the registry (i.e. have a certified business relationship with the registry, and be capable of receiving certified resources from the registry).

- A resource transfer would commence by having the resource disposer lodge with the registry a digitally signed intent to dispose of an address, and the resource acquirer' to lodge a similar signed intent to acquire this listed resource.

- On receipt of both signed intents the registry would lock the resource against any simultaneous transactions and issue each of the parties a "transaction key half" and a validity period for the key (which becomes the validity period in which the transaction must be completed), the resource to which the transaction refers to and the names of the parties, signed by a verifiable registry key. The registry is committing to undertake the registration transfer of this resource between the two parties on the condition that

both halves of the "transaction key" are deposited back to the registry on or before the expiration of the transaction validity period.

- Presumably the two parties would engage in a transaction that saw the acquirer have a third party validate the transaction key halves and then taking control of the disposer's transaction key half in exchange for some form of consideration, and the acquirer subsequently returning both transaction keys to the registry to complete the transaction.

- If both transaction key halves are returned to the registry on or before the time when the transaction validity period expires, then the transfer is undertaken by the registry by performing a database resource revocation from the original holder and a database resource allocation to the resource acquirer.

Admittedly there are still many details to work through here in developing a model of how resource certificates could be used to underpin IPv4 address transfers in a reliable and robust manner, but it does appear that such digital instruments could play a very useful role in this context. If address scarcity is going to give addresses inherent value, and if the realization of transfer policies provide a legitimate opportunity for this value to be realized, then the need for a clear title to the "right-of-use" is an essential prerequisite, and in this space resource certification appears to provide a clear solution.

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

About the Author

GEOFF HUSTON is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. he graduated from the Australian National University with a B.Sc, and M.Sc. in Computer Science. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for the initial build of the Internet within the Australian academic and research sector. He is author of a number of Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005, and served on the Board of Trustees of the Internet Society from 1992 until 2001.

http://www.potaroo.net