PRAGUE – ASO/NRO Presentation on RPKI
Wednesday, June 27, 2012 – 12:00 to 12:30
ICANN - Prague, Czech Republic

CHAIR DRYDEN: So welcome to the ASO NRO. We are pleased to receive a presentation from you now on the issue of RPKI. There's been various interest from some GAC members to find out more about this issue, and I know a it's something that the community has been working on, the numbering community.

So I will hand over to John Curran who will introduce himself and his colleagues.

JOHN CURRAN: Good afternoon. I'm John Curran. I am the chairman of the Number Resource Organization, the NRO. The Number Resource Organization also serves as the ICANN Address Supporting Organization.

I also have with me at the table the chair of the Address Supporting Organization Address Council, Louie Lee. I also have the CEOs of the RIRs that make up the Number Resource Organization who are here, including myself for ARIN, Raul Echeberria for LACNIC, Paul Wilson for APNIC, and Adiel -- Adiel, I'm not going to get it right, Adiel Akplogan for AfriNIC.

We also have, to present regarding RPKI, we have the chief scientist of APNIC, Geoff Huston, who will take it from here.

Thank you, Geoff.

GEOFF HUSTON: Thank you, John, and good afternoon, everyone. This presentation is a highly technical presentation insofar as it does cover technologies that we're not normally used to seeing so overtly.

It covers technologies that relate to the security of our infrastructure in communications.

Can I have the next slide, please.

Interestingly, there are many ways to be bad on the Internet. There are many ways to do bad things.

You can certainly try spewing out lots of spam, and folk do. You can try and corrupt the operation of the DNS system, and the DNS is under constant attack. And you can also try and send very particular packets to machines to make the machines do something they were never intended to do. And they're very much the same as biological virii. They are viruses. They change the operation of the system they infect.

But there are other attacks which are even more insidious. Those attacks don't try and change the operation of your machine. In fact, as long as your machine is working perfectly well, the attack is more successful.

These two kinds of attacks are attacks not on individual machines but on the infrastructure of the Internet itself.

The first in the Domain Name System has been a topic that many of us have been familiar with for many, many years, and the efforts to put forward solutions around DNS security, DNSSEC and its deployment, is,

as we see here in this ICANN meeting, well under way. Many workshops, much activity, and much understanding.

Routing is different. Routing is a very, very hard problem.

To understand how to direct each of those packets to their intended destination actually requires the operation of some of the more sophisticated algorithms we've ever built and deployed. Routing is an extremely difficult problem, even in terms of its underlying technology.

When we first built routing systems, and I'm going back almost 40 years to 1960, the early '60s, it was done in a research environment, and research environments tend to make massive assumptions. And one of the assumptions was that everybody is an honest and straightforward player. Everybody has the same motivation. And the routing algorithms are based around -- that screen has just gone black -- are based around models of mutual trust, which are very important for the Internet.

Mutual trust is no longer an environment we live in. But how do we count on mutual trust? If we don't accept that everyone is a good player, what is the response?

The response is that everybody has to check everything. But that check function is extraordinarily difficult because each and every player who routes then needs to assemble a large amount of information all the time about addresses and routing policies. There is no centralized repository of such information, no well-understood techniques that apply across the entire Internet. It's an extremely difficult job.

So instead of doing that, we've gone down a solution which has been cost efficient. And cost efficiency has said there's some vagueness at the edge. Things happen. The system is insecure.

There have been some notable incidents in the past. I'm sure many of you who have followed the area of security would be well aware of an unfortunate incident for a few hours one evening a couple of years ago when an ISP in the Asia area managed to block access to YouTube for the entire planet for a small amount of time. These things happen.

Most of the incidents we see are typically a result of finger trouble. It's just things go wrong and they propagate over the network.

But today's mistakes are often tomorrow's vulnerabilities. But if it's possible to do it by accident, it's possible to do it by intent.

So we have to understand that the system we're working in is not good; that your own systems might be perfectly secure, your own laptop might have all the updates there, the Web might be perfectly fine, everything else is working, but if the routing system has been compromised, your packets will not go to their intended destination. They might pass through a few unintended way points or not get to the right destination at all.

Next slide, please.

Obviously we can't look after every packet. Packets aren't like that. There are way too many.

Obviously we can't equip routers with people behind every one of them. There are way too many. We need to look at automated systems,

systems that operate at the same speed as the packets that run through them.

What we need to be able to do is actually put a discriminator in our infrastructure that allows us to detect and exclude attempts to put false information into the routing system. We need to be able to tell good from bad automatically.

There are very few basic tools that do this in a public system. As anyone in cryptography would tell you, it's easy to create remarkably secure one-time cryptographic pads, but the Internet isn't like that.

It's easy even to create cryptographic systems when the two parties who are going to exchange information meet beforehand and exchange secrets. We don't have that system.

We have a system where the parties who are trying to exchange this information will never meet and can never meet. That limits the choice of tools we have to a very small set, and that very small set is actually public and private key cryptography.

So what we're using is actually conventional digital signatures which is signed by a private key where only the public key can unlock that resulted digital artifact.

The next thing to look at is how do we send the public keys around the network? How do we distribute those credentials? How do we inject that trustable authority into the network?

Next slide, please.

So what we need to understand is, firstly, how do we describe trust? I have an address. Oddly enough, my IP address is just a number. 3, 10, 1,000,020. How does the rest of the world know that that number, that IP address, is valid and genuine and is Geoff's? Because for the Internet to work, every address must be unique.

We have a system that actually uniquely allocates individual addresses all the way down to end systems. It's the address allocation network, that hierarchy that starts with the Internet Assigned Numbers Authority, IANA, then the regional address registries, and then potentially national Internet registries, local Internet registries, and all the way down to end machines.

So my number is unique because APNIC gave it to me. And APNIC's number pool is unique because IANA gave it to APNIC.

If we can describe that chain, that will give us the credentials to create trust in the addressing system.

So what we're trying to do here is not introduce new data. We're trying to reformat the registry to allow authentication members to be built on top.

Next slide, please.

So this, then, leads us to the concept of a resource certificate. A certificate is actually quite an old artifact in our world. The X.509 standards for digital certificates date back some decades, and this is one more application of that same common standard.

It's a digital document that basically binds together some number resources and a public key. And it's signed by the certificate issuer's private key. So all of a sudden you now have an artifact that can validate that when Geoff signs something to say this address is mine, any of you can figure out whether I'm lying or not, whether what I'm saying true, whether you can authenticate my assertion.

So we think this is actually pretty powerful. And certainly I would say it's not something the RIRs just invented on their own. We have been working in this space together as RIRs and in the Internet Engineering Task Force since 2006 in building both viable technologies that hook together and the underlying standards that then allow folk to build and operate.

So it's very much a community-driven approach.

Next slide please. So this is perhaps another way of publishing the same registry data we always publish. It's a format that is subtly different because now these are X.509 certificates and holders of resources can opt in to generate a digital certificate that attests to the fact that their key pair is uniquely associated with IP addresses and it's derived completely from the underlying registration databases. So the certificates and the databases reflect precisely the same information. Next slide.

So now we have this next concept, and it's a bit like the domain name hierarchy. In this case it's a hierarchy of digital certificates which is known in the security world, because they love inventing new terms, always use a new term whenever an old term could have done just as well, instead of using hierarchy they like the words "Public Key

Infrastructure," PKI. So this is a hierarchy of certificates that talk not about my identity, not about my role, not the conventional things digital certificates talk about. These are digital certificates in a hierarchy that talk about IP number resources. So this allows statements such as "I am the holder of a particular address" to be digitally signed and for anybody else, anybody else to check whether that assertion was true or false.

When I say anybody, I mean anybody or anything. Even any router. Even any switching element inside the network itself. Even any command control interface for standard network operational support. Because you can say things that directly relate to how addresses on the Internet are originated and routed. I, Geoff, the owner of 1.1.0/24 -- and I am -- I can authorize AS23456 and only that network to originate or route to me. The corollary is, if anyone else tries to highjack my address, not just me, I know they're lying, but everyone else in the room, everyone else in the Internet, knows they are lying, too. It's much harder to tell lies when everyone knows they're lies. Next slide.

This is a new development for us. Routing security is extraordinarily difficult and the community have had long debates as we push this forward. We're certainly aware in a number of regimes that there's been some interest in digital certificates and some interest in legislative regimes that allow judicial systems, courts, to revoke certificates under certain circumstances. Typically they refer to identity or role-base certificates, conventional certificates. But the community has certainly had discussions around the issue of the issue of being forced by a Court to revoke or otherwise alter a certificate. We have no answer for this, but we do observe the same judicial process could just as easily direct a registry holder, the owner of that registry, the operator, to change the

contents of the registry. Revoking a certificate, changing a registry content, is actually much the same issue. So I would certainly say we haven't got a solution but we have neither introduced nor reduced the factors around this issue of external pressures on the integrity of the entire registry system.

It's a hierarchy. Like the DNS, it's a hierarchy. If you manage to compromise close to the root, the effects flow down to enormous parts of the infrastructure. If it gets compromised high in that hierarchy, the damages and the potential risks are enormous. But that is similar to compromising the certificates used by Visa or MasterCard. And if you think about chaos, think about if they were compromised. Many of today's digital systems, well outside coms that underpin huge amounts of our economy, have exactly the same issues. And the industry has done a remarkable set of standards around ensuring the integrity around the operation of certificates. FIPS standards, that essentially try and make the keys completely tamper-proof. We use industry-based practice in managing these keys. We can do no better. But we certainly use the best we can possibly do. So our systems of key management and certificate issuance are up to the absolute top in terms of industry standards in this area.

There's also an issue of resilience. Many systems fail. Automated systems have failure modes. But the current system, particularly around the area of publication of policies, actually relies on the existence of a unique place where those policies are lodged. And it's where you got them from that gives them integrity. Signed data is different. If it's signed, everybody can publish it. And anybody who gets any copy can tell instantly if it is a faithful, accurate, and complete copy

of the original. Digitally indistinguishable. So the certificate that I produce and I sign, each of you can take a copy and republish. Republish. And anyone who takes that republished artifact can be assured it is exactly the same as the original bit by bit. So yes, there are issues of failure, but at the same time this kind of signed information we think gives us a lot more resilience inside the underlying infrastructure. Next slide, please.

So where are we? We're certainly deeply down this track because the routing system is a vulnerability and the Internet is important and it is under a lot of pressure. We are moving with determination and some speed in getting this through. On the certificate infrastructure side, a number of RIRs have already integrated this into their production systems. Members inside those particular communities can generate these certificates as they desire right now. Other RIRs are still working with their communities to complete their implementations. It is a lot of high expertise work and because there are some differences in implementations going around there, certainly some RIRs are doing things subtly differently and they will be ready in the short-term future. So we are integrating this into production. We certainly would like to see all RIRs finish this very, very quickly.

Certificates aren't everything. You need to integrate them into existing operational support systems. We need to have apps. A bit like other systems, we need apps. And we are certainly working with many folk, not just the RIRs but in the IETF and other industry and in some public bodies around generating plug-in modules that use this. And also the issues of how to distribute and synchronize this information about the validity of every address and every route across the Internet every

second. In other words, making sure that this data is complete and accurate all the time. At the same time, over in the IETF there is work still underway in securing the actual interdomain routing protocol itself, PGP. We've gone a fair way down there and we've certainly got through a number of issues around session integrity and origination integrity. And we're now biting off the bullet of I think one of the hardest ones which is actually securing that very tricky thing called an A.S. path which is actually a chaining in security sense which is causing us a certain amount of pause to think. But the technologists are certainly optimistic that between the technology curves of Moore's Law, more efficient use of encryption algorithms and more common knowledge and practice of cryptography in our community we will solve this as surely, I think, as we've solved the problems we've met so far. So we are confident that we'll be able to achieve this in the near future.

So I think with that -- next slide -- I have, yes, gone through as much as I think is appropriate here and we'd all be happy to answer questions you may have. Thank you.

CHAIR DRYDEN: Thank you very much. I see New Zealand.

NEW ZEALAND: Yeah, thanks, Geoff. That's a very, very interesting presentation. I guess the obvious question for the GAC is, are there any public policy impediments to achieving this? Is there anything that the GAC can do to assist, speed up the implementation of the -- of these protocols? Thank you.

GEOFF HUSTON: Certainly some governments -- some sorry national bodies have been very aware of the nature of these problems and have been extremely active in supporting research and development and certainly agencies in the United States have been engaged with this for many years, but that's not the only institution and the only -- the only country. We certainly see many other countries be aware of the problem and support activities around this area. So that's a good thing.

We do have this issue of we don't operate through the terms of immunity from judicial and legislative environments. And the communities have certainly, when they have looked at certificates, expressed deep concern over a law court, for example, ordering a certificate to be revoked because the implication of that revocation is not just they don't have that address. It's that that address' certificate for routing disappears. That means the entirety of the presence of that address and everything lying behind it disappears for everybody else. And in introducing security you introduce these other factors which are novel factors in some cases. I'm not sure I have answers, I'm not sure I'm looking for answers, or anyone at this point, but in terms of things to discuss in a public policy forum, this is certainly one of them.

CHAIR DRYDEN: Thank you very much. Did you want to reply as well, John, and I see Paul as well.

JOHN CURRAN: John Curran, President and CEO of ARIN. With respect to encouraging deployment, it's important to recognize that the decision by a service

provider to make use of RPKI and to securely announce their routing information or their routing policy to some extent, is voluntary. Service providers decide that they're going to participate in RPKI because by doing so, their routing information is less likely to be compromised by others. Likewise, they decide to pay attention to RPKI information so that when they're receiving routing information they're less likely to receive incorrect or suspicious routing information. So the choice to publish using RPKI and then the choice to pay attention and look at that on the receive data is both voluntary decisions.

In the ARIN region is Canada, the United States, and 26 economies in the Caribbean. I'm aware in the U.S. that there is an Internet reliability group sponsored by the FCC. It's an industry best practices group. They've actually brought service providers together to talk about best practices in routing security as a voluntary practice.

So there are ways of looking at this, but it is not something that the RIRs require anyone to do. We are the natural location to provide the infrastructure for this, but the use of it, both in publication and in looking at the receipt of data, is an ISP voluntary decision.

CHAIR DRYDEN: Thank you. Paul, you wanted to add?

PAUL WILSON: John covered it very well. A couple of other points which may help this to be understood is to see the -- the existing system is one in which the RIRs are providing the registration details of the addresses that we have allocated and the holders of those addresses. The certificates, in some

sense, are to extend that registration record with a signature. In the same way that an e-mail can be accompanied by a digital signature that tells you that it -- it came from where it claims to have come from. So the opt-in process which John referred to is -- it's important to see that by voluntarily opting in what a service provider is choosing to do is to both publish the signatures for the records that it holds in one -- in one half of the equation and then in the other half to make sure to respect signatures that it receives. So this is a system which has evolved in a way that's entirely compatible with the bottom-up opt-in consensus-based process of the RIR system itself rather than something that is being imposed top-down. And I think one of the -- one of the reasons for coming here and making this presentation is that we felt that although the system has been under development for quite some years through the standards process and then the support that the RIRs have developed for it has been under development also for some years, we find that the questions about the system are starting to be propagated out more widely and that we felt it was useful for the GAC to have this update on how the -- how the system works and to ensure that there's a good common understanding, in particular of the opt-in nature as opposed to a kind of a -- an imposed system which it has -- it may have been described as in the past. Thanks.

CHAIR DRYDEN: Thank you very much, Paul. Okay. So I have Portugal, Norway, Malaysia, and the EU Commission. So Portugal, please.

PORTUGAL: Well, thank you very much. First of all, the clarity of the presentation, it's a somewhat tricky technical issue and it was certainly presented in such a way that we can understand.

I was aware about the system from RIPE efforts. Now, my question goes somewhat along the lines that already started by New Zealand. So given the GAC's role it would be interesting to know what you think should be things that we can do, either regarding advice to the Board on anything related to this, which -- to be clear, I don't see where that stands, or policy adoption at national levels or raising awareness. So it would be nice if you could make clear what somehow governments can contribute to this extent. Thank you.

CHAIR DRYDEN: Thank you, Portugal. Raul, were you going to reply?

RAUL ECHEBERRIA: Yes, thank you, Madam Chair. I think that's the main purpose for the NRO to come to the GAC and bring this issue is just to -- to let you know what we're doing that's governments are aware. I think that this is an important change for the Internet and a version that as Geoff said we have been working on this version for many years and we have made a huge investment in time of working, money. This is something big for the Internet. It is important that the governments are aware of it. I think that's probably the main way in which you can help, if you -- if this is what you want to do, is to create awareness, as you say, in the local -- in the local -- with the local industry as John, for example, said. We

have an example in U.S. and this is a good thing to do in other countries, too.

CHAIR DRYDEN: Thank you, Raul. So I have Norway, Malaysia, EU Commission, Uruguay, and U.K.

NORWAY: Yes, thank you very much, Madam Chair. And thank you much, Geoff, for that presentation and the update on this PKI system that, as you said, had been going on for some years. So I think that's also important, I think, for us as governments to know about this system because it can be a very important security measure on the Internet as such.

I would also like to comment on some of the questions that raised about the public policy issues. I think also -- I think this issue here is about what we can do is, of course, awareness raising and also best practices in the different regions of the world and we have different regulation in the different parts of the world. In Europe, which Norway's a part of, and of course we have powers as a regulator to impose security measures on the ISPs if we see that as a good thing to do.

So in our -- we act on communications in Norway, then, of course, we can, actually, mandate this for the Norwegian ISPs. But, of course, I think this was something that will develop and will be a best practice between the ISPs around the world. And, of course, with the Internet, you cannot apply measures in isolation. You know, this is a worldwide system. So I think that's important to do.

One question of the more technical -- but that's -- two questions, one technical question and one on the timelines.

When is the system operational? When has the applications, routers, software, everything updated? And when is the standardization to have this implemented in BGP finalized?

And the other technical question I have is the certificate issuing. Are the RIRs going to have self-signed certificates which then they use to sign the resources with? Because I think some concerns from some governments -- not our government, from other governments, is that, if all the RIRs' certificates are going to be signed by one other certificate controlled by someone else, that can sort of be -- if that then certificate is revoked, you will then just crash the whole -- everything on the Internet. So, in that respect, I think it is -- I'm interested in how the chain of trust is going to be built within this RPKI system.

CHAIR DRYDEN: Thank you, Norway. So, Geoff, you'll reply.

GEOFF HUSTON: I'll start with the first of your questions, which was the easiest. And then I'll pass it over to John here who will address the remainder.

What I wanted to, I suppose, highlight here is this issue when you said about best practices versus a regulatory requirement about the deployment and use of this kind of technology, it is true in DNSSEC that, if I have Geoff.potaroo.net, whether I sign it or not is irrelevant unless potaroo.net unless dot net are both signed. There's a hierarchy here in

DNSSEC. In the routing system we don't have the ease of a hierarchy in routing. If an island of routers does secure BGP and then has to pass that routing information through a section of the Internet, that does not implement that form of BGP. All security information is lost. And, when you get back to another island that supports it, it isn't there. We cannot easily do piecemeal deployment of secure BGP as a protocol in terms of getting the maximal amount of benefit. Oddly enough, this is one of those systems where, if we all did it, the resultant benefit would be universal and it would work. If islands do it or if it's done in a piecemeal fashion, the benefit that results in terms of what parts of the Internet are secure and for whom in a routing sense, that benefit is much reduced.

So you might want to think carefully about this issue of what is secure best practice in infrastructure at a national and regional level and think carefully about how you wish to maximize that but, at the same time, not impose prohibitive costs or high risks to the existing operational environment. So I'm not saying there's a clear answer. But, again, there's certainly part of an agenda in a public policy process at a regional and national level as to what is the most appropriate way to engage in a technology where piecemeal deployment is not as effective by a long way. It's not as effective as universal deployment.

CHAIR DRYDEN: Before you continue, John, if I could just suggest that there be a long form given of BGP and a bit of context around that. Not everybody is familiar with the standards related to this. Thank you.

JOHN CURRAN: Ah, yes. So I'm John Curran. And I'm going to pick the three other implied questions that were in your questions.

So the first one I guess I will pick up is that regarding timeline, each of the RIR has its own timeline for deployment. And that's for the infrastructure for the digital certificates, whether that's issuance or linking to service providers who are issuing. And that timeline, I will say, the other RIRs are well ahead of ARIN. And we are the laggard here. As it turns out, the way that liability works in our region is such that we have to take extreme care to make sure that we can associate our digital signature activities with organizations in a way that does not allow repudiation, in other words, that we can absolutely confirm that the ISP asked for the certificates. And that requires more work on our part. So we're probably the laggard. And we're looking at a timeline between now and the end of this year for the end of our production services. Most of the other RIRs have production services available today. And so it's just a question of waiting that small amount of time.

With regard to the certificates that the RIRs use and the anchoring of what we call trust, or a trust anchor, RPKI allows someone relying on that information to configure a trust anchor, a digital item in their system. So, if you have a routing -- set of routers and you're an ISP, you could configure each of the five regional registries' trust anchor. And you would believe things issued by the five RIRs and what's below them.

It's also true that it would be convenient to have a single global trust anchor. And, in fact, the Internet Engineering Task Force, the IETF, the IAB, the Internet Activities Board, over that issued a recommendation calling for RPKI to be deployed with a single global trust anchor, if at all

possible. We're working towards that goal, working with ICANN. We had, actually, very productive meetings this week with the team leader, Elise Gerich. And, to the extent that that's something that proves workable, then we will also have the ability not just to use RPKI with five trust anchors but to have a single global trust anchor that includes the resources of the RIRs plus resources such as reserved resources, reserved IP addresses for special purposes. So the good news is that these are individually configured. So, to the extent that there is an issue, a party relying on a single trust anchor could configure a single RIR or deconfigure a single RIR from what they feel like they want to trust.

I guess the last item I will pick up briefly is, when it comes to -- I heard the term "regulation" and how that can help, I guess there's a step before regulation in terms of advocacy.

Many governments themselves are users of ICT technologies. You have your own networks and your own systems. To the extent that you want service providers who have secure routing and participate, you should ask that as a customer. That's a good way to spur deployment and interest in these technologies.

I'm not saying there's not a public policy issue beyond that. But I don't want to omit that intermediate step of you as a customer of ICT saying you want certain quality in your service providers and you want them to use secure routing. Thank you.

CHAIR DRYDEN: Thank you, John. Malaysia, you're next, please.

MALAYSIA: Thank you, Madam Chair. Thank you for the introduction of this technology. I would like to say that it interests me. Because at the moment we have a lot of challenges in promoting DNSSEC to our ISPs. Although we are regulating them, but we want them to volunteer. And because of it's voluntary, I think I believe you understand that the uptick is very, very low.

So I would like to -- I really am interested in the timelines and your outreach programs to us so that we can bring this technology and try to promote it to our country and to our ISPs. Thank you.

CHAIR DRYDEN: Adiel, would you like to reply, please?

ADIEL AKPLOGAN: Yes. In terms of timeline, as John mentioned, we are all working together to have the same timeline and be ready together. And I can say that we have already all of us launched the platform for having a signed certificate for resources already, for having a self-signed certificate. So that means that the system is already there, and people who want to use it can already use it. I think the objective of the presentation today is to raise awareness among the GAC so that you can start doing this awareness locally from ISP to start -- using the system to start playing with it. And we have also had a good support from some equipment vendors who have already integrated this technology in the IOS, routing IOS so that it can be really used in the real world of the Internet today. Yes, the uptick will be slow because it's a new thing

being added to the curve. But it is already there and we should start making people use it as soon as possible.

CHAIR DRYDEN: Thank you for that reply. Okay. So I have the EU Commission, Uruguay, U.K. And then we will move to close this session. So, next, EU Commission, please.

EUROPEAN COMMISSION: Thank you, Madam Chair. And, to echo what our colleagues have said, many thanks to the presenters not only for being here and discussing making the technology understandable to everyone, which we understand that's not an easy task. So thanks for that.

I have two questions which can be answered by whomever of you wants to answer that. Concerning the choice of trust anchors, who in particular I speak would choose to trust in this system? Only regional Internet registries can be trust anchors or also other entities can be trust anchors in this system? Is there any particular requirement for any entity to be a trust anchor or to provide this kind of service to Internet operators?

And the second question: It was at the beginning of the presentation, so I may either have misunderstood or I may not remember well. But at a certain point I heard someone, I think it was Mr. Huston referring to the fact that the community had concerns about the possibility that a law court would issue or take a decision implying the revoke -- I think revoke was the term -- used of a digital certificate using the RPKI system.

Now, on this specifically, I would like to know if you can explain which are parts of the community are having that doubt or those concerns, whether there have been cases of law courts doing that or there are ongoing cases or there is any reason to believe right here right now that this can happen shortly.

Now, of course, we, as the European Commission we're not going to make any kind of comment on what law court does or does not. It's not our job. But it would be interesting to know if this is already happening or this is just some hypothetical concern just like the kind of hypothetical concern that we, as public authorities, are often accused of putting on the table. This may happen so you shouldn't do this. So thanks for the clarification.

GEOFF HUSTON: Thank you for those questions. Who can be a trust anchor? Let's sort of wind this back a little bit and ask a more basic question. Who can issue certificates that attest that some other party holds a resource?

Well, in theory, anybody could. But whom should you believe? The party that issued the resources is perhaps the best party to issue that certificate. So, if APNIC issues an address block to a local Internet registry, then the certificate issued by APNIC is the one that you would probably do best to trust.

And another digital artifact called a certificate issued by someone else perhaps shouldn't be trusted. So the trust model has been deliberately aligned very precisely with the address allocation model. And, while it is always a case in secure systems that folk who use them can pick any

trust model they like, certainly, we would recommend that they use a trust set that corresponds to the agencies that allocate the resources in the first place.

Whether you use a trust set of the material issued by each of the five RIRs and use five entities as your trust model or whether you use a single trust entity pushed out that describes the root at IANA is up to you. But perhaps it would be unwise to replicate what we did in browsers that have more than 150 points of trust and more than 700 different entities. Because that's way too many.

So, certainly, a much smaller number is better, but it doesn't have to be one. As to your second question about the discussion of concerns, I think it's reasonable to report that those concerns were aired -- in a most detailed sense inside the European area in the RIPE forums. And, unfortunately, Axel is not with us today to describe that further.

But there were cited in that community instances where, in a different space for different reasons, there was the orders relating to revocation of certificates for other purposes by law courts.

And the concern was voiced in the community, wow, do you really think that this could also apply to digital certificates? We would like to think not. Because the certificate is merely a mirror of the underlying registry content. And, revoking a certificate doesn't really change the registry, per se. It just makes life more difficult. And I'm not sure that was of the intent of such processes.

So we'd certainly like to think that, as we go through this process and understand more about the integration of digital certificate and

cryptography into this kind of infrastructure, the rest of societies's institutions and tools come along with us and appreciate their own roles and responsibilities with respect to this. Gratuitous revocation does not help here. Thank you.

CHAIR DRYDEN: Thank you, Geoff.

Uruguay, please.

URUGUAY: Thank you for the interaction.

I don't know if I missed it, but I wanted to understand how this infrastructure relates to the local -- the national public infrastructure. I mean it -- not only by the technical point of view, but also in the legal point of view. You know, in each country the legal value of the certificates and all the -- how do you say in English? All the confidence of the -- of the -- of the system, of the infrastructure relates to parties that -- to certificate authorities that are empowered to give certificates by regulatory unit.

So in a way, the legal aspects of the national public infrastructure is related to some kind of adequacy and how this relates to each other. Perhaps there is some kind of compatibility or not. I don't know.

Thank you.

JOHN CURRAN: This is John Curran, and you ask a legal question and I am not a lawyer. Having said such, in the process of exploring the aspects of providing RPKI certificates, it turns out that each country has its own framework for the legal validity of a digitally signed document, and that means that the RIRs, in issuing these certificates, we make sure we take care that we know the meaning of these digitally signed documents and we believe in that meaning. That meaning talks about the holder of a number resource or what that holder believes is the entity that's allowed to route that address block.

And so in some countries, I am sure that there is national jurisdiction that make those certificates equivalent to signed documents, effectively, issued by the registry.

This has implications for the registries issuing those documents and causes us all to use a high degree of care in running the certificate, but it is not universal. It is very much a country-by-country situation, and so I can't give you the general answer.

I can say that it is something that service providers in countries who issue these certificates need to understand they may be issuing documents with the same strength when it comes to a legal system.

CHAIR DRYDEN: Did you want to follow up?

URUGUAY: Yes, please.

The thing is if you -- if the ISP has any legal responsibility for not -- for wrongdoing as an ISP, the legal framework he will be working on is the national legal framework. And this legal framework is regulated by these national laws, and these national laws have their national public infrastructure.

So for one of the questions as was made here, what are the things that the GAC can do and work around, is trying to perhaps have some compatibility between the national frameworks and this in order to provide a legal extent to working with the ISPs at the local level.

But I think we need some more interaction from you in order to know how to work in our own countries.

JOHN CURRAN: Agreed.

CHAIR DRYDEN: Raul, please.

RAUL ECHEBERRIA: Yes. Just for adding some elements. This is a super IDN infrastructure, and the certificates that are issued under this framework are with the only purpose of being used for routing.

So there will not be any transaction using those certificates. So the ISPs will not use those certificates for making any transaction of any kind at the local level. So there would not be any legal responsibility on that.

They will use the -- this information only for knowing if the -- if the network that is announcing a block of IP addresses on the Internet is the one that has the authority for doing that or not, and it will permit them to take a decision on routing. Nothing else than that.

So those are -- those certificates will not be used in any country for any purpose that is regulated under the legal frameworks of each country.

So that's the -- I don't know if this answer is enough.

URUGUAY: In the case of the ISP couldn't misuse the rules to make harm to the network.

GEOFF HUSTON: If I could again very briefly respond here, there are many kinds of digital certificates out there. Some are used in the Domain Name System to underpin https onto its Web sites. Others are used to attest to the identity of citizens of a country.

Conventionally you find that the certificates that are under the highest amount of regulatory interest, national interest, are certificates that attest to identity and role of people. But certificates can do a lot more than that, and the ones that we are working in are very much similar to the certificates used in the Domain Name System relating to the association of a domain name with an IP address to do secure Web servers.

Conventionally, such certificates do not directly fall under individual national regulatory frameworks, per se. Conventionally, in many

frameworks, they fall under an industry practice of issuance and maintenance.

We would certainly see these certificates that did not attest to identity and do not attest to role but associate a key peer with the holder of a number resource as being a reflection of a technical artifact as distinct from a role.

And as such, I think, would fall more in the regulatory area that talks about technical artifacts and technical issues like domain name certificates as distinct from identity or role certificates.

So again, I don't see the level of regulatory interest in this to the same as other forms of certification.

CHAIR DRYDEN: Thank you. I think we'll have to move to our final speaker and I hope this exchange will continue off-line, and I think this is a topic we can take up again in the future with you in the GAC.

So I have U.K., please, and then we will close this session.

UNITED KINGDOM: Thanks very much, Chair, and thanks very much for the presentation which very usefully complements the briefings we've had from -- in Europe for the European governments, as Luis from Portugal referred to, the briefings we've had from RIPE NCC on this issue. And it's a reminder that secure routing is still a goal for the community, and we certainly hope that goal will be achieved.

As I recall from the European briefings, it was apparent that not all the industry was in line, you know, as I think you have been sort of touching on in some of your responses. I'm talking about the ISPs, of course.

And I guess for those of us in government, we have to keep a watching brief here, if the industry is not -- not totally speaking with one voice.

And so when it comes to what we can do to promote awareness, we're a bit sort of one hand tied behind our back in that respect. So, you know, okay, common, industry, get together and find a way forward. And I know RIPE NCC has got ongoing work in this area, and we'll, no doubt, get further briefings in Amsterdam when we governments meet up again with them.

And I hope the other RIRs are also, likewise, briefing governments on this critical issue. I expect they are.

But anyway, in the ministry, I will steer my technical advisor, who I run to on issues like this, I'll steer him to this -- to the transcript of this, and there may be sort of technical points I follow-up on as a result of that.

For me, a couple of very basic nontechnical questions. Firstly, is the expansion of the Domain Name System of thousands of, possibly, gTLDs over the next ten years or so, however rounds there might be adding sort of critical urgency to this work, so that's the first question. And then, secondly, is wider deployment of RPKI going to have a significant impact on reducing criminal abuse of the system, of the DNS, is the second question.

Thanks very much.

GEOFF HUSTON: Thank you. Let me, again, respond to those two questions. The first one is of course delightfully simple. The answer is not at all. Names and numbers certainly work distinctly in this case. And the expansion of the namespace in terms of its structure in the new gTLDs has no bearing whatsoever on this resource PKI. They are completely separate strains here and there is no relationship.

The issue around the escalation of insecurity on the Internet is certainly an interesting topic. 15, 20 years ago, insecurity was the product of adventurous 16-year-olds who had nothing better to do of an evening, and we have seen insecurity now become an industry. A criminal industry, but an industry.

Certainly with the value of transactions on the Internet, subverting the normal operation of the Internet is of interest to players who are not legitimately playing, who shouldn't deserve our trust.

Attacking routing is a valid attack, and can be, with sufficient knowledge, capability, and resources, an extraordinarily effective attack. You can attack individual points in the network or wide-scale areas. You can dial exactly the effect of an attack in routing.

This is not a comfortable situation. And certainly these measures to secure routing are not done because we have nothing better to do next Wednesday. It really is because of the pressing matters of agenda and certainly insecurity. Infrastructural insecurity is the worst possible problem for us. Everything else might be working fine but if the infrastructure -- if the train tracks are going to the wrong destination, the train will go there anyway.

So we see this as being critical. We certainly see widespread deployment as having a mitigating factor on the potential ways that the Internet can be subverted for what is, in effect these days, largely criminal-based activity or other forms of activity that don't deserve our trust.

So, yes, this is important.

Thank you.

CHAIR DRYDEN: Thank you very much.

So I thank you, as always, to the ASO or NRO for coming to present to us on this topic. We've gone well over time, but there was such a level of interest that I did not want to prevent the discussion from continuing longer.

So I do hope we can return to this topic again in the future, and, again, thank you.

So for the GAC, we don't benefit when we have short lunch breaks, so I'm going to suggest 2:45 to return, and then we will continue with our agenda at that time. 2:45.

Have a good lunch, everyone.