# Transcript of Press Conference
# Inaugurating PCH Cyber Security Facility in Singapore

Wednesday, June 22, 2011, 14:30-15:30 SST
Swissôtel The Stamford, Singapore

**Brad White**: My name is Brad White, I'm the Director of Global Media Relations for ICANN. We'd like to thank everybody joining us online as well as the journalists who are here in the room. We're here today because we have an announcement regarding a special cyber-security center that's going to advance DNSSEC. I'm not going to talk about that because the gentlemen who are speaking are the experts, and they have a far more compelling narrative than I do.

Allow me to introduce the folks who will be addressing us today: Marcel Schneider, Manager of Special Operations for SWITCH; Jeff Moss, Vice President and Chief Security Officer for ICANN; Bill Woodcock, Research Director of Packet Clearing House; Tommy Hor, Director of the NUS Computer Center; Lim Choon Sai, Director of Internet Resource Management, Infocomm Development Authority of Singapore; and James Kilaba, Deputy Director of the Tanzania Communications Regulatory Authority.

Jeff, let's start with you, if we could, please.

**Jeff Moss**: All right. Thank you, Brad. I'm Jeff Moss, the CSO of ICANN. ICANN, in one of its many roles, is tasked with ensuring the security, stability and reliability of the Internet's unique identifiers. So, as part of that, ICANN has been very involved in the policies and the deployment of DNSSEC in the root zone. We encourage other gTLDs and ccTLDs to deploy DNSSEC as soon as technically possible, because we believe DNSSEC is very important in both enabling future innovation and enhancing the overall security of the domain name system. As part of that, at the beginning of the year, we had about zero zones signed. Just last week, last month, we had about seventy zones signed, and just on Monday, the 20th, through the work of Packet Clearing House, fourteen more ccTLDs were signed, raising the total number to over eighty-five. If we stick with this trend, we're hoping, by the end of the year we'll have the vast majority of all zones signed, which will be a fantastic achievement, to think that we've gone from basically zero to almost 100 percent in one year, once DNSSEC's adoption began.

So, I would like to thank and congratulate Bill Woodcock and Packet Clearing House for signing these fourteen new zones. I think it's a very positive achievement, and it's one that I hope to be congratulating others on in the months ahead. So with that, I'd like to introduce Bill, the Research Director of Packet Clearing House.

**Bill Woodcock**: Packet Clearing House is a not-for-profit organization that has focused on building secure Internet structure for the past eighteen years. We have built more than one hundred Internet exchange points, and we host more than eighty top-level domains on our global DNS infrastructure. So, when Rod Beckstrom asked us last year about the feasibility of building out DNSSEC infrastructure on top of that, it seemed to be a natural fit with our mission, our staff and our capabilities. We have since been building infrastructure to do this.

Our service is interesting in several ways. First of all, it's operational and providing services right now. Secondly, because of our non-profit nature, it is done at no cost and it is done openly in the sense of open-source, with Creative Commons licenses of all the documentation and legal work that's being produced. Our goal is not so much just to sign a bunch of top-level domains but to do the knowledge transfer necessary to allow top-level domains to sign themselves, to operate their own infrastructure. So, we just try to make this happen, we don't try to control the process. All of the work that's being done is open for anyone to take, use, or emulate, however they wish to.

Specifically, we're building three physical security facilities. The first one here in Singapore; the second one in Zurich, Switzerland; and the third one in San Jose, California. These follow the same model as the root. We're using the same physical security, we're using the same procedural security, we're following the same standards that ICANN does in the process of signing the root. The point behind that is that auditors have to be satisfied with the way the root is signed, because the root is not going to be signed different ways for different people. If we use the same processes and procedures as the root, then the auditors can be assured that they don't have to compare apples and oranges, they don't have to look at different standards, they know that the root signing process and the TLD signing process are the same. The sole significant change between the way the root is done and the way our service is done is that the root is signed in two locations in the United States. We sign in three locations, two of which are outside the United States in very neutral countries.

With that, I'd like to introduce Lim Choon Sai, who is at the IDA, the Infocomm Development Authority of Singapore, which is our local host for the physical security facility here in Singapore.

**Lim Choon Sai**: Thank you, Bill. The Infocomm Development Authority of Singapore, or IDA, and the Singapore Network Information Center, or SGNIC, are very pleased and honored to see this node of Packet Clearing House's DNSSEC platform hosted in Singapore. We are grateful to NUS for hosting the facilities. When PCH contacted the Ministry of Information, Communications and the Arts to request that the facility be hosted in Singapore, IDA was more than happy to facilitate the process. DNSSEC is very important, as users are able to gain assurance that information returned by the remote DNS server they are seeking to communicate with is independently verified and genuine.

IDA and SGNIC established a task force in 2009 and recommended that DNSSEC be implemented to strengthen the security and trustworthiness of the DNS infrastructure for secure and safe usage of .sg domain names. Singapore is already gearing up to be ready for DNSSEC implementation in a number of areas, which will not only assure the Internet community of Singapore's commitment to curb abuses of DNS but also instill confidence among the industry and the public that .sg domain names are secure and trusted. Today we are happy to see the establishment of the facilities at NUS, which will assist other countries to secure their DNS infrastructure. Singapore is committed to the security and well-being of the Internet, and we look forward to exchanges with the Internet community in other possible ways to do so.

Thank you, and I would like next to introduce Tommy Hor. Tommy is the Director of the NUS Computer Center.

**Tommy Hor**: Thank you, Choon Sai. First of all, I'd like to thank IDA for approaching NUS for the hosting of this facility. At NUS, the birthplace of the Internet in Singapore, we provide neutral ground in terms of business as well as politically for hosting such a facility. We're very pleased to be able to contribute our expertise and work with the agency and partners to develop this cyber-security infrastructure. More important is that today, when we surf the Internet and we're supporting so many billions of users, one of the concerns is always about the genuineness of websites. This facility will provide us a more secure way of assessing information on the Internet. Of course, the physical security of the facilities involved is important, and we hope we can contribute to this great initiative and we can help with everyone of the institutions and organizations in terms of securing the information on the Internet.

Thank you very much. With that, I can hand this over to Marcel, who is the Manager of Special Operations at SWITCH.

**Marcel Schneider**: Thank you very much, Tommy. For me it is very easy to say that we are very delighted and honored by Packet Clearing House's decision to host a zone-signing server at SWITCH in Switzerland — in Zurich. You probably all know that Switzerland is quite a stable and well-connected country. So we will do our best to meet your stringent requirements. And all I can do is thank you very much again, and all the best for your company and for all the projects you will do in the future. With that I'd like to hand this over to James Kilaba from Tanzania.

**James Kilaba**: Thank you very much. I would like to introduce the .tz registry, as it is very new to you and this will be an opportunity to be known. The Tanzania Network Information Centre, tzNIC, was established in the year 2006 and incorporated in Tanzania as a non-profit entity. Its role is to do the management and administration of the .tz domain and its associated secondary level domains. The founding members of tzNIC were the Tanzania Communications Regulatory Authority and the Internet community through the association which is known as the Tanzania Internet Service Providers Association (TISPA). The Centre became operational in August 2009, and in April 2010 the Centre was designated by ICANN as both Administrative and Technical contact for the .tz country code Top Level Domain.

tzNIC is designated to promote the utilization of .tz domain names, protect registrants' interests and ensure affordability and security of domain names for unique identity of Tanzanians in cyberspace. The Centre has just finalized its first strategic plan, which is due to start on the first of July of this year, in which DNSSEC implementation has been given priority. So, the strategic plan is of this kind [displays printed strategic plan], and it will be operational on the first of July.

Originally the Internet was designed without much security consideration. Instead, it was designed to be a scalable distributed system. That design has been successfully operational, and we don't complain about that, until recently when DNS-related vulnerabilities were detected and exploited. These vulnerabilities have forced the innovators to think about security. That's why the current global agenda for ccTLD domain names to be secured on the Internet has been a call for them to implement the DNSSEC chain of trust. Of course, because .tz is part of the DNS hierarchy, it would never be exempted from that.

Coming to the relationship between tzNIC and PCH: tzNIC is enjoying anycast DNS service provided by PCH to its TLD, .tz and seven other second level domains. This service therefore gives .tz presence in more than thirty locations globally. So, to us, that is a good thing from PCH.

On the DNSSEC deployment, using the PCH platform, we all know that DNSSEC implementation presents a lot of challenges. That is obvious, including the cost of deployment and the management of the keys. In the event of trust leakage, what could happen is that the key management presents a security risk, as keys are uncertainly secured, seldom changed, or shared among users. So, in addition, data can be made inaccessible or, in the worst case, of course, can be permanently irretrievable if the keys are lost or damaged. This is the obvious thing, but we are not afraid of those because the solutions are there. I, myself, witnessed Monday's key ceremony and how secure the process of creating and storing the Tanzanian keys was — very strict. But that said, again, it remains all vested in human trust.

Nevertheless, because of the DNS Anycast we enjoy at tzNIC, we have a partnership with PCH, and as a step towards securing the Internet, implementing DNSSEC using the PCH platform is currently considered as an easy undertaking, as PCH already has .tz zones. As of now, the .tz zone is already signed on test mode, which is currently available for our engineers to test and to familiarize themselves with the platform. It is therefore important that tzNIC grasps the expertise and gains knowledge of key management through this good arrangement which is tailor-made by PCH. We thank very much PCH for deployment of this.

Finally, I would conclude by saying that our future plan is that we have chosen this for learning purposes because of the good research process which is being conducted by PCH. But the full deployment and adoption of DNSSEC using the PCH platform will of course depend much on the results obtained from this testing, which is going on well, and with other political considerations as may be appropriate. With that, I thank you very much.

**Brad White**: Great. Thank you, gentlemen. We can take questions now from the journalists in the room. Just raise your hand and I'll call on you. And if you would be so kind as to just click the button on the microphone so that they can hear you online. And for those of you who are online, there's a place you'll notice on your screen to be able to type out your question, which we will get. The first question is online. I'm going to split this question in half between you, Jeff, and you, Bill.

Jeff, for you: For the journalists who have not previously covered this arena of DNSSEC and its role in cyber-security, is it an oversimplification to say that it eliminates, or does it simply minimize, the chance that Internet users will be misdirected to a site that they didn't intend to go to? In other words, clarify exactly what DNSSEC is doing.

**Jeff Moss**: When you query the domain name system to figure out from a host name to an IP address, to resolve where you want to go, in the past that's all been done over UDP, a mostly insecure protocol, with no cryptographic verification that the result you get is actually the result that's intended by the name system. So essentially with DNSSEC what we're doing is moving to the majority of queries coming back over TCP. It will be harder to spoof, not impossible but harder. But the most critical component is that they'll be cryptographically signed. So you have much higher confidence. I'm not going to say it's a hundred percent secure, because that gets security people in trouble. But it is a much higher confidence that the answer you get is actually the answer that was intended. And that's a first.

**Brad White**: So if I can clarify for the person that wrote in, it's an extra level of assurance that you ended up where you wanted to go.

**Jeff Moss**: Precisely. And the interesting thing with this, from my perspective, is that this — I alluded a little bit earlier to innovation — this is going to allow people to do new things that they had not intended, that had not been possible before. When you didn't necessarily trust the answer that got back to you, you would relate to the name system in one way. But if you have higher confidence in the answers you get back, you may now start relying on DNS for more. And I think we already see people writing articles and talking about what other new innovations are possible. And that's the part that is really exciting for me, the transformation of the way we interact.

**Bill Woodcock**: I think any time there's an increase in the level of law and order, the level of assurance, in a system, you find new uses and people become comfortable relying more upon the Internet or upon any substrate for things like commerce and banking and so forth. I think this has been one of the weak points of the Internet over the past ten years — that there have been continuous upgrades and security flaws, and it's been a cat-and-mouse game in the whole banking and online commerce sector. So finally having a protocol that is not really subject to this kind of half-measure back-and-forth is really a huge step forward.

**Brad White**: And Bill, can you explain in lay terms exactly how the opening of the Singapore center will advance that layer of security, advance the DNSSEC movement.

**Bill Woodcock**: In the past, before DNSSEC, the answers found in the domain name system were simply assertions: someone said that the answer was this, but you weren't able to tell who made that assertion. Theoretically the right person did. But if the wrong person had made that assertion, you as an end user would have no way of knowing that. So this opened the door to a number of kinds of attacks, DNS spoofing attacks, that were often used in compromising people's banking credentials and credit card fraud. What DNSSEC adds is a cryptographic signature that allows the user to know that the person making the assertion is the person who is authorized to do so — that it is your bank telling you where to find your bank's website, not a random Eastern European cyber-criminal. Specifically, this facility is a hardened physical facility with five layers of physical security surrounding a set of cryptographic keys that are being held on behalf of, at this point, fourteen ccTLDs, but presumably many more as we go forward in the year.

Responsibility for the cryptographic security and the physical security is divided into two non-overlapping groups of people. For the physical security, two of three people must be there to unlock the safes, the doors, and provide physical access to the facility in order to use it. In order to use the cryptographic functions, to do key signing, depending on what the function is, either five or three of a group of seven trusted parties must be present. So in the signing that we just did on Monday, five people — I think most of whom are here in the room with us today — joined us, each one with a share of a cryptographic key that was necessary to activate the equipment that does the key signing. That, in simple terms, is what happened here on Monday. We used a physically secure device to generate cryptographic keys on behalf of Tanzania and thirteen other countries, to sign their ccTLDs, their country code top-level domains.

**Brad White**: We do have another online question, but any questions from the journalists in the room?

**David Goldstein, Goldstein Report**: What will Internet users actually see as the result of it? You said they will see a more secure net with banking and things, but when they are just browsing the Internet, what will they actually see?

**Bill Woodcock**: Google has just announced a new version of their browser Chrome that uses DNSSEC to visually indicate the security of a website that you've browsed to. All of the other browsers are on track to do the same thing. People's email software, over time, will also use DNSSEC. And eventually all Internet applications will be upgraded to utilize this additional level of security. In the meantime, if someone is suspicious, they can use many online sites to manually check the validity of a DNSSEC signature.

**Chua Hian Hao, Straits Times**: How big is the NUS facility and how many staff do you have? Also, what is the cost of the center?

**Tommy Hor**: It doesn't require a very big facility in terms of the space. Basically it's a box running by itself. In terms of staffing, all the operations and support is provided by PCH, and they can do that either remotely or on-site. So, in terms of facilities, in terms of footprint, it doesn't require a lot of space. The cost of it in terms of constructing a facility — I'm talking about the physical space — is in the region of SGD 20,000, but that cost is excluding the equipment and all the other facilities.

**Bill Woodcock**: I think it's fair to say that the system overall, including all the space and so forth, is several million dollars. Obviously a huge portion of that is the physical space that's being used in each of these secure facilities. So we are greatly indebted to Marcel and to Tommy and to Equinix for the facility in the United States, because theirs is probably the single largest contribution. ICANN has supported this by giving us moral support, by giving us the idea in the first place, and by seconding one of their staff and part of his time in the last year to provide the expertise and help us understand how exactly the root was done so that we could replicate that in an open-source way.

As Tommy said, the physical facility is very small, only two meters by three meters. All three facilities are identical. They have exactly the same equipment in them. And so inside that two- by three-meter room is a SCIF — a secure compartmentalized information facility — which is essentially an even smaller metal room that locks up tight. And inside that is an IPS, an information processing system security container, which is a safe. And inside that is an HSM, a hardware signing module. So this is five layers of physical security, each one more difficult to penetrate than the last, and each one requiring a greater level of authorization to access.

**Vivian Yeo, ZDNet Asia**: When will the other two facilities be ready? Jeff mentioned earlier fourteen ccTLDs. How many of them are from Asia?

**Bill Woodcock**: Let me start with the timeline. The San Jose facility is operational and has been operational for the past three months, but of the five layers of physical security, only four are completed so far. The same thing is true of the Singapore facility. The Singapore facility has been operational since Monday of this week, when we did the signing. But again, only four of the five layers of physical security are complete. The fifth layer of physical security will be finished in August. For the other two facilities, we're aiming for September for the Zurich facility and October for the San Jose facility. Regarding the number of TLDs that are in Asia, I would need to go back over the list, but one is in central Asia and there are a bunch in the Pacific islands. So far it has mostly been fairly small countries. One of the reasons James is here with us is because Tanzania is not only the second most recent country to join the system but also the largest country to join the system so far.

**Soon Weilun, Lianhe Zaobao**: I have three questions. The first one would be, what is the benefit of having three different locations? Number two, are you looking to expand the facility if more and more domains join this network? And number three, you mentioned five physical layers. Is there a reason why there are five and not four?

**Jeff Moss**: On your first question, if you look at the history of the domain name system, it's a distributed system. It's gained a lot of its strengths and resiliency from having many components spread across geographic regions. It allows for faster responses from a local geographic region. It allows isolation in case there is a natural disaster or man-made accident. So I think, from our perspective, the more facilities the better. It adds to the overall resiliency of the domain name system. From where I sit, I would be nervous if everything existed in one facility. I like the idea of a distributed model.

**Bill Woodcock**: To follow up on the first question, because the users of the system are national governments, and national governments often have little reason to trust each other, if this facility were hosted in any one country, there would be some subset of other countries in the world that would not trust that country. Therefore, we chose three different countries which are not particularly aligned with each other, and all of which are relatively trusted by many other countries. Now, every time a signature is done, it is compared between the locations. And if any location does not agree with the others, we throw an error — we publish the fact that there was a difference, and that's made public for the world to see. If, for instance, the United States government decided to tamper with the results of the signing, the Zurich and Singapore results would be different but they would agree with each other. And that would be made evident for the world to see immediately. Therefore it serves as a deterrent to any government to tamper with the system, and it serves as an assurance to other governments that the system is secure and is not being tampered with. It's transparent. So that's the reason for three facilities. We could of course do more facilities, but the facilities are very expensive to operate, and we think that three is a reasonable compromise. We were asked two weeks ago at the AfriNIC meeting in Dar es Salaam why there was not a facility in Africa. And honestly the reason was simply because our budget is limited and we needed to choose three locations, and we went for three that had the ability to support us through donating the facilities and were in highly trusted countries.

Moving on to the second question, are we looking to expand the facilities as we add more ccTLDs. The physical facility need not expand. Another very minor difference between the root and our system is that, although we are using the same manufacturer's hardware signing module, we're using a faster model of it. The root, because it needs to generate only a small number of keys, and only infrequently, every few months, has no stringent performance requirement. We, because we are signing these zones constantly — every few seconds we're issuing a newly signed zone — we have to have the higher-performance model. So, as we add more domains, if performance requires it, we will parallelize by adding more of these hardware signing modules. The hardware signing module is made by a British company called AEP. The model is Keyper. It's also used by many banks and financial services institutions.

Moving on to the third question, I'm going to refer it back to Jeff because, again, PCH is emulating the root, as exactly as we are able to, in order that auditors from countries that want to use the system will not have to learn and understand two different systems. So, Jeff can answer why the five layers.

**Jeff Moss**: Because the facilities, the root-signing facilities, are in the United States, they were modeled after the highest level of security, based on U.S. federal standards — FISMA high security. And so a lot of those standards came out of the Cold War and military, sort of worst-case thinking. So that's why you see so many overlapping layers of security and physical controls. And so, to make the U.S. government comfortable with our standards, we emulated what they thought were the highest levels of security and what would give us the highest level of assurance. It's sort of like we followed them, and PCH followed us. And also, the U.S. government spent a lot of time and money working out the kinks and debugging these systems over decades. So it's not something we just invented. There is a long history behind why these decisions were made.

**Harry Suhartono, Reuters**: So is it possible for two countries to collude and tamper with the system and make it, the process, appear to be genuine relative to the one who is not involved?

**Bill Woodcock**: Hypothetically, anything is possible. And as a security person, one never says that something will not or cannot happen, because that is tempting fate. Part of the reason why we chose Singapore and Switzerland and the United States is because these are countries, particularly Switzerland and Singapore, that have a long reputation of neutrality and of independence. And so first of all, we try to minimize the likelihood of such an occurrence. Secondly, we try to maximize transparency. So, if two countries, tried to do that, it would be very apparent. In each facility there are three video cameras publishing continual video surveillance of the SCIF to the Internet. Anyone on the Internet can observe all three facilities at all times to see that no one has gone into the room and laid a hand on the SCIF. If someone were to get to the SCIF, they would then have to open it and get to the IPS inside that. If they were to get to the IPS, they would have to somehow open that and get to the HSM. If they got to the HSM, then they would need to compromise at least three of the seven trusted people to get the cryptographic key material that activates the HSM. Otherwise, even shaking the HSM will just cause it to erase all of its contents. And again, that is made public as it happens.

**Jeff Moss**: And the other thing is, since these sites are constantly cross-checking each other, if you were to make a change, you would have to do it at the exact same moment. Otherwise you would see that one country had changed it, then another country changed it, and you could put together the order in which this occurred. So, if you were trying to make it look like a third country changed it, you would see this time disparity.

**David Goldstein**: Jeff mentioned that you can do things not possible before. Could you give an example of some of these new things that would be possible with DNSSEC?

**Jeff Moss**: Well, I can just speculate, because some of these things aren't being done. But, for example, now that responses are coming out of the DNSSEC-enabled servers over TCP, packet sizes are larger, responses can be bigger. And there is already work being done in the IETF and some other fora on extensions. There's a proposal for a DANE extension, allowing you to publish your own SSL certificate within the DNS response. But from my perspective there's no reason why you couldn't publish other information in the DNSSEC. So right now you ask a question — Who is QQ in China? — and you get an IP address back. But there is no reason you couldn't ask for a recipe for dinner and get that answer back. Or ask for a photograph of a cat, and get that back. There's a lot of data that you could store, potentially. And I think we're at the very beginning of this innovation. And I think the domain name system will be doing many things it was not really intended to do, a decade from now. And from my standpoint, that changes the risk model. Because all of our models were designed on IP addresses, but yet now it will be doing more. And I find that very fascinating.

**Bill Woodcock**: I would like to second Jeff's response about DANE. DANE is probably the single most important follow-on from DNSSEC. DNSSEC itself is a building block, and it provides a hugely useful increase in security of DNS lookups, of getting answers to DNS queries — but beyond that, using it as a building block to enable a higher level of security for web transactions and for voice-over-IP. If you wanted to authenticate a phone call, there's no reason why you couldn't use DANE. And there is, in fact, a standards effort to use these building blocks — DNSSEC, DANE on top of that, and then SIP on top of that — to secure a SIP telephone call over the Internet, a voice-over-IP telephone call. And I think what you'll find is that, as these building blocks come into popular usage, the things at the top of that stack of blocks are impossible to guess at now. We look back five or ten years ago and many of the things on the Internet that we take for granted now were not predicted then. So, it's very difficult now to look forward and say what will come from this fundamental building block.

**Jeff Moss**: I always like to point out, imagine how much more business would be done, how much more innovation, how much more communication would occur, if you could trust your email. If I could trust the email from my bank, and not fear that it's a phishing attack, or if I could communicate with my local government or my school — just imagine how much more people would have confidence. And so, what we're seeing now with DNSSEC, and IPv6, is that the fundamental foundation of the Internet is getting an upgrade. We've been working toward this for more than a decade. These next ten years are going to be a very transformational time on the Internet, because not only will you see DNSSEC and you'll see IPv6, there is some other work going on in routing. The foundation is being built in cement now. It's not going to shift under our feet nearly as easily as it has been. And that will enable a whole new generation of applications and trust, to do things I would never in my right mind do today. But ten years from now, absolutely.

**David Goldstein**: Can you foresee any link between the announcement of the approval of the new gTLD program and any new gTLD possibilities and DNSSEC, or is that sort of a bit too pie-in-the-sky, at least at this stage?

**Bill Woodcock**: I'll take the liberty of giving an answer, but really that's an ICANN question. Specifically, there is a document that ICANN has been working on for some time specifying the technical requirements for new gTLDs, and one of the technical requirements for new gTLDS is, I believe, that they at least have a plan for deploying DNSSEC in the short term. Rick, is that right? [Rick Lamb nods agreement] Rick Lamb is the DNSSEC program manager for ICANN and is the person who assisted us in getting this off the ground.

**David Goldstein**: Just to follow up, though, will it change any possibilities of use — like, for instance, as a new way of doing a contact database? Would DNSSEC change what a new gTLD might do? Or you just can't tell for now?

**Bill Woodcock**: There are certainly new gTLDs that have as part of their business model been counting on DNSSEC. For instance, there is a financial services TLD that will probably apply — that will have a very strong chain of trust all the way through from each bank to the end user, using DNSSEC. So, yes, that is integrated. It doesn't particularly have to do with our platform, however, which is ccTLD-specific at the moment.

**Brad White**: I'd like to relay one question that we got online. Mr. Woodcock explained the country-selection process, but, Mr. Kilaba, what does it mean to your country to be one of the first to make use of the new Singapore DNSSEC center?

**James Kilaba**: We in Tanzania always join innovations. We like innovations. And because DNSSEC has been a global agenda, we don't want to be left out. As Bill has put it, the selection of all the countries are very fine to us, we don't have any problem with any country of the three. As of now, the testing is ongoing, and we don't have any problems. So, that's what I could say.

**Brad White**: Alright, if we have no more questions, gentlemen, thank you very much. I want to tell the folks in the room as well as the people joining us online that we will very shortly, on the press page of the ICANN website, have an audio recording of this news conference. And if you guys want to go back and hear anything, it will be up and posted on the press page, ICANN.org/press. We'll have a video recording of the news conference posted and uploaded as soon as we can do that. Gentlemen, thank you very much for your time.

**Bill Woodcock**: I should also point out that there is a backgrounder for the press with quite a lot of technical Q&A, as well as Q&A about DNSSEC and the process we followed. And it also has contact information for a number of independent experts in the field who have agreed to speak with the press. And that will also be up on PCH's and ICANN's websites.

## Addendum: Additional questions submitted online

**John Markoff, New York Times**: Why would it be important to authenticate a voice call? Don't you know whether you're talking to the person you think you're talking to, by recognizing their voice?

**Bill Woodcock**: Four reasons. First, it would provide authentic caller-ID, before you picked up the call, allowing you to better distinguish friends-and-family from telemarketers. Second, it would protect against man-in-the-middle attacks, though not against passive wiretaps. Third, people often receive calls from people they don't know, representing organizations they may have heard of but have no way of knowing whether the individual actually represents; authentication would let them know whether they really were getting a call from the President, or whether it was a prank call. Lastly, as technology improves, I imagine voice-synthesis and artificial modulation will improve as well, and it may become more difficult to distinguish people by voice. Already, we've seen reduction of voice channels from 64kbps clear-channel to CODECs that run over as little as 6kbps, often with corresponding degradation of voice quality and resiliency to packet loss. Market pressures have pushed downward on least-common-denominator service over the past twenty years, and that's sometimes not even enough information to be able to accurately assess the gender of the person on the other end of the line, much less know who they are. The combination of voice masking and spoofing technologies with lower-information-rate channels may make authentication of calls from people you do know more interesting as well.

**Dugie Standeford, Warren Communications News**: What are the ccTLDs that have signed up to this program?

**Bill Woodcock**: The ccTLDs that are already signed are:
.af (Afghanistan)
.cx (Christmas Islands)
.fo (Faroe Islands)
.gl (Greenland)
.gs (South Georgia and the South Sandwich Islands)
.gy (Guyana)
.ht (Haiti)
.ki (Kiribati)
.nc (New Caledonia)
.nf (Norfolk Island)
.sb (Solomon Islands)
.tl (East Timor)
.tz (Tanzania)
.ug (Uganda)

Of those, New Caledonia is the first to declare themselves “in production” by putting a DS record in the root zone. Also there are a number of other ccTLDs in different stages of testing, and many of those ccTLDs also include second-level domains that are signed as well. Things are changing fast. It was only ten a week ago.

As you can see, this project is very much aimed at assisting countries that might otherwise not have an easy time of getting DNSSEC implemented themselves.

**Dugie Standeford:** Are others in the process of joining?

**Bill Woodcock**: Yes, two others began the process today. We currently host more than eighty TLDs on our anycast DNS platform, and we expect we'll see similar overall uptake on this service. This service is brand-new though, so countries are just now finding out that it's available.

**Dugie Standeford:** Other than having set up its own DNSSEC, why might a ccTLD not wish to participate?

**Bill Woodcock**: Mostly it's a matter of autonomy and self-reliance. We're doing this as much to help countries do it themselves, as to host them. So we're not "keeping score" in the sense of trying to get a lot of them to use our platform, we're more interested in seeing them signed, generally, than just signed by us. Knowledge-transfer is a huge part of this project; we currently teach about ninety workshops all over the world each year, and we've added DNSSEC trainings (largely in developing countries), with the goal of helping countries understand the technology, and see how they can do it themselves at a lower cost than we (and the root) are doing it.

So, to answer your question, a country might wish to generate their own key-signing keys, and use those to generate zone-signing keys, which they would give to us to employ in signing their zone many times a day. That would allow them to have complete and sole control over the cryptographic portion of the work, while "outsourcing" the expensive operational and network security portions to us. Alternatively, they might just wish to use all of the legal and process-development and software work that we've done, which we're publishing open-source and under a creative commons license, and implement it all themselves. If they choose to skip some of the more expensive physical security standards that we and the root are doing, they could save many hundreds of thousands or millions of dollars, while still having a reasonably secure system.

**Dugie Standeford:** If DNSSEC is provided free of charge to ccTLDs, who actually pays for the program, centers, etc.?

**Bill Woodcock**: PCH is a non-profit, and all of our services are provided at no cost to the recipients. Our costs are met through donations from a variety of sources; Prior to this program, we had a $9.5M/year budget, and including this, nearly $12M/year, of which about 60% is met through donations from the Internet industry private sector (companies like Equinix, Afilias, Cisco, NTT, Level3, Neustar, and others), about 30% from governments (France, Denmark, the United States, Chile, Singapore, Canada, and many others), and about 10% from private and intergovernmental foundations, like the Soros Foundation and the United Nations Development Programme.

This particular program is being paid for in part out of our general fund, and in part by the donations of the secure site hosts, specifically the Singaporean government (IDA specifically), SWITCH, the Swiss research and education network, and Equinix, a commercial datacenter operator. If you calculate the net-present-value of the facilities being donated, the project overall is requiring about $55M in donations to make happen, though the actual amount of money being laid out at the moment is very small by comparison with that; less than $2M in present spending to get the project off the ground.

**Monika Ermert, Heise.de**: How is the project funded, you spoke about a 2 mio budget (mainly taken for setting up the physical infrastructures, and borne by the institions on the table)

**Bill Woodcock**: It's a little hard to calculate. The budget for the facility build-out and the equipment and the staffing to-date has been less than US$2M. If you calculate the net present value of the donated facilities, however, from IDA, SWITCH, and Equinix, that comes to just over $55M. I don't think any of them are thinking of it in exactly those terms, but this definitely wouldn't be happening if they weren't donating the space, and that amount of space walled off in a first-rate datacenter is immensely expensive over time. I only found this out yesterday, but before NUS stepped forward and volunteered space in their datacenter, IDA was already negotiating with Certis for space in their vaults, and they were going to be paying roughly US$30K/month for that. The Zurich and San Jose spaces would be even more expensive, if we were not receiving support from SWITCH and Equinix.

**Monika Ermert**: How much does operations cost per TLD, if you can say that?

**Bill Woodcock**: At present, we're only offering the service to ccTLDs, and we do not charge any fees for it. If you were to divide the overall ongoing cost (about $2M/year) by the number of ccTLDs using it, at the moment, they'd all be getting a $140K/year service for free. If as many ccTLDs signed up for this service as have signed up for our anycast service so far, our per-ccTLD cost would drop to less than $20K/year. So you can see that it's very efficient for us to host as many ccTLDs as possible on it, because it amortizes the high expense among as many beneficiaries as possible. There's very little cost that scales as a function of the number of ccTLDs on the system… Almost all of the costs are overhead for the program as a whole.

**Monika Ermert**: How much do TLDs joining have to pay for the service?

**Bill Woodcock**: ccTLDs pay nothing.

**Monika Ermert**: Would you recommend the distributed signing structure for the root?

**Bill Woodcock**: That's a political question rather than a technical question, and I understand why the U.S. government desires to see the root signed entirely within the U.S., but in the long term, it's hard for me to imagine the process not being distributed and done in parallel in several countries, in the same way that we're doing for ccTLDs. In general, I believe that it's ICANN's destiny to become even more international in nature than it is today.

**Monika Ermert**: Who and how are the persons keeping key parts selected, by you or by the respective TLDs?

**Bill Woodcock**: At the moment, the seven people holding key-parts ("Crypto Officers" or COs) are:
Kim Davies
Steve Feldman
Lim Choon Sai
Jonny Martin
Michael Sinatra
Stephan Somogyi
Gaurab Upadhaya

The three people holding physical access ("Security Controllers" or SCs) are:
Bob Arasmith
Lee Han Chuan
myself, Bill Woodcock

We use a five-of-seven COs control for HSM operations, and a three-of-seven COs control for simply generating new ZSKs, however the seven COs have no way of using or abusing the keys that are generated, since they're encrypted with a key that's only shared across the four HSMs, and the two HSMs that can generate keys cannot sign zones, while the two HSMs that sign zones cannot generate keys. The COs only have access to the two HSMs that can generate keys, and not to the two that can sign zones. In all cases, physical access control requires two-of-three SCs.

The trusted parties have all, to date, been selected by PCH with input from the community, using a mix of PCH staff and others who have realm-specific knowledge and are well trusted by the community. We consulted broadly, and ran these people through an informal-but-thorough process. And we'll certainly be rotating other people in over time. This list is definitely not set in stone; it's better not to have people become fixtures in positions like this.

Going forward, yes, we anticipate continuing to work with our constituent ccTLD administrators to settle upon a good balance of trusted parties. Bios of the COs are included in the press backgrounder.

**Monika Ermert:** Can new gTLDs also use the service?

**Bill Woodcock**: At the moment, we're doing it for ccTLDs and national IDN TLDs, and we're open to not-for-profit regional and cultural TLDs, like .cat, as well. In a year, when the new gTLD question becomes more pressing, we may open it up to at least not-for-profit gTLDs, but this is something we're not yet committing to. If you look at the way we operate our anycast service, I think you can extrapolate how this service might be operated five or ten years from now.

**Monika Ermert:** Uptake of DNSSEC signatures on second level has been slow, so how about registrars in developing countries - how did they react so far?

**Bill Woodcock**: Yes, that's definitely an issue. I had a long conversation with the Congo-Brazzaville regulator on exactly that topic this morning… I think organizations like CoCCA and NIC.BR will probably be helpful there, in getting open-source registry-registrar code out there that fully supports DNSSEC. In the mean-time, there are plenty of larger registrars that support DNSSEC, but I fully understand that many developing country markets don't want to be dependent on those large, US-based commercial registrars.

Ultimately, though, I don't think this will be much of an issue. The technology always looks daunting at first, but there are infinitely more smart kids out there writing code than I ever predict, and my worries rarely turn out to be justified.

-end-