COPENHAGEN – DNSSEC Workshop -- Part III
Wednesday, March 15, 2017 – 13:45 to 15:00 CET
ICANN58 | Copenhagen, Denmark

JULIE HEDLUND: Thank you again for joining part III of the DNNSSEC Workshop. My name is Julie Hedlund. I'm with ICANN staff and I'll go ahead and moderate the last segment of this workshop. In doing so, I would like to say that I'm very pleased to introduce our next presenter. This is Vittorio Bertola. He is from Open-Xchange and he'll be talking to us about Trusted Email Services. Welcome, Vittorio.

VITTORIO BERTOLA: Thank you. Thank you very much for the opportunity to explain what we are doing. This is actually my first DNSSEC workshop. I used to be a regular at ICANN meetings 10 years ago but it's been a while since I last came. I didn't really know what to expect and I did a mix of what we're doing and the real technical problems and then maybe in future occasions we can go into more specific issues, but as for the first time, this is sort of a general description of what we do. Next slide please?

We deal with e-mail. We are basically an e-mail and DNS software company and so one of the issues we noticed is that e-mail transport is really not secure as of today. Actually people

who are in the sector already know this but if you go to the average user, the average user usually thinks that e-mail is really secure, it goes around the network encrypted and protected and authenticated, but it's not really like this.

Actually today the encryption and the authentication of the e-mail transport seems really insufficient and the industry as a whole has a responsibility in this because in practice this allows massive stopping and interception of everyone's e-mail. Even if, as we know, e-mail is still the communication way of choice for the most important data and documents in everyone's life, usually the wholesome feedback that users don't really care about security, they don't even know this and it's a very technical matter. But what's happening in the last two, three years is that the public has gained a really great perception of the issue and of the problems related to e-mail security.

Next slide.

This is just one. If you think at it, it would be unimaginable that an entire country will be discussing in the middle of a presidential campaign whether e-mail was managed securely or not. Actually, this was and still is in the U.S. making headlines for several months now but this is just one of the cases in which e-mail security issues went observed by the public so made the news. There were several cases, of course, but—next slide—

there's even situations that are maybe less well-known but are more worrying.

These are two articles from British newspapers. You may just still discount them but they are reasonably serious newspapers and they tell the situation of two different people that were cheated while selling their home because their e-mail was intercepted. Someone in some way could either read the e-mail between them and their agent when it was being transmitted or break into their e-mail account and the result was that they were wired the wrong bank transfer coordinates for the bank transfer and they lost significant amounts of money.

So it's really a matter of general security not a matter of geopolitics and spying and whatever but really a mail of every day security for the people. So what do we do here? What are we trying to do?

Next slide.

What we see is a real literal entire e-mail ecosystem because if you want to secure e-mail, either you have a closed system or a system in which you expect everyone to have an account like Google or Facebook is now, otherwise you can secure e-mail transmission only by cooperation so e-mail will go from one ISP for the sender to the ISP of the recipient and so there's at least

two different operators involved. So you cannot have security if you don't have cooperation.

Another option is that if e-mail doesn't get secure, most people will move their communications to chats, instant messaging and whatever. It's already happening today and the problem I have with these systems is they are really proprietary and closed often so they're not open standards like e-mail and so we risk really to end up with an Internet which is made up of closed gardens, wall gardens and proprietary code.

Next slide.

There are efforts everywhere. I think some people here are aware of this but I wanted to mention that some governments at least are starting to take seriously the issue and they're starting to make recommendations. The German one was already mentioned this morning by someone else so the government is requiring e-mail providers to adopt DNNSEC and DANE and there's also other governments doing this including the U.S. And also more importantly there are efforts by the providers alone.

Next slide.

This is the German one so also in response to the pressure by the government, all the major e-mail providers in Germany now use DNSSEC and DANE [inaudible] authenticated the exchange of e-

mail and the transport of e-mails among them. And then they even made this other marketing point so they actually advertised so that the usuals are aware that communications between two German e-mail addresses even if they are measured by different providers are more secure than ever at least.

So we saw this project and we thought at it and it's Open-Xchange. We are in a good position to spread the word and so we decided to put some energy and resources for the good of e-mail in general to spread this idea to other countries.

Next slide.

This is what we call TES. It's just a name we made up but what we mean is that there should be some general standards to secure e-mail. And so especially Telcos ISP hosters, people who have millions of e-mail addresses often should try to deploy the technologies that are there but unfortunately not everyone is using [Yetro], very few people are using.

Next slide.

I was asked also by the Program Committee whether this is just an initiative of Open-Xchange. Open-Xchange which now is the parent company also of Dovecot so basically it's the 72% of the

world's e-mail servers on our software, on our servers and probably DNS as well.

So of course as being one of the leaders, we felt a responsibility. It started as an idea inside a company but now we're really trying to broaden the reach and this is also why I'm here now. We have involved other vendors. [inaudible] secure are two vendors of e-mail related software and services and we would like to build momentum behind this.

I know that there are other efforts, for example, by Isaac trying to push these technologies. We are in a nice position because we have several customers among the biggest telecommunication operators in Europe and also outside of Europe. What we do is that we can really spread the word and together with anyone else who wants to join try to educate the operators to adopt technologies.

Next slide.

Actually, this is what we do. It started with a set of technical guidelines that would help making your e-mail secure which include, as we will see, DNSSEC and DANE and we started with a model in which we would basically invite the operators in a given country to a meeting. We would have closed meetings, we're still having them. We had eight or nine of now.

We invite both the technical and the marketing people running e-mail services from these companies and we explained to them what the threats are and what the open standards to solve them are, and if you're very surprised even the technical people don't really realize all the risks that are there and they ask for more. They start thinking of how to solve these issues.

So of course we have a mailing list. We even have a closed Facebook group because unfortunately people like to use Facebook but now what we're trying to do is also spread the world beyond the operators' community. So we're addressing independencies as means in smaller ISPs and whatever. And what we are doing is we set up a website and we try to explain again what the DANE and DNNSEC is and other technologies and convince people to adopt them.

Next slide.

This is a sector of technologies we recommend. Of course we will not go into all of these. The typical test meeting takes some two hours and a half or three hours so we'll just briefly mention now for—I'm sure that people around the table know how you can use DNSSEC and DANE to secure e-mail. Some of these people are actually those who invented this but maybe in the audience not everyone knows. I also wanted to show exactly why DANE is so important for securing e-mail transmission.

Next slide.

This is a recap of what happens when you actually send e-mail over the Internet. The two MTAs, the two e-mail servers from the originating and the receiving provider have to start a dialog and what happens is that the receiving MTA will say that they accept encryption because unfortunately, as we know, the encryption in the e-mail transmission in the SMTP is entirely opportunistic so it's not compulsory. And also the other problem is that you don't really know whether the receiver will support it so it's the receiver of the test to ask for it. So usually the receiving MTA asks for encryption and so the sending MTA says, "Okay, let's start TLS," and the traffic is encrypted.

But what happens—next slide—is that this is easily subject to many [intermedial] text so if someone can intercept the communication, they will just receive the STARTTLS indication from the receiving MTA and filter it out. They will tell the sending MTA that there's no encryption supported and what happens is the sending MTA will just fall back on clear text communication. So the e-mail will be sent in clear and all the communication will be intercepted and this can then be forwarded to receiving MTA so there's not even a way for the receiver to realize that they are being intercepted.

Next slide.

And then also another way you have to attack or intercept e-mail is to use the classic cash poisoning attack against the DNS. So when the sending MTA that we follow opening the communication has to look for the MX record, the sending MTA will receive a wrong MX record which has been manipulated by an attacker and so will establish a communication with a recipient which apparently is the right one but in fact it's the attacking one. And the recipient could even provide a valid certificate and authenticated and whatever. The sending MTA doesn't have any way to realize that they are sending e-mail to the wrong destination. And even if it's encrypted it will just be decrypted at the other end. DNSSEC and DANE, the technologies that can really prevent these two types of attacks from happening.

Next slide.

I don't think we have to explain what DANE is, do we? But the two points I would like to make is really that first DANE is really good for e-mail encryption because it provides a trust time code that is not depending on a certification authority. This is important because we've seen the difficulties in keeping all certification authorities secure. Even if just one certification authority gets cracked then the cracked certification authority could emit value certificates for everyone.

But even more importantly, the really important thing that it does DANE is to provide a way for recipients to communicate that they really want to receive encrypted e-mail or else not receive anything. So the real problem in the standard is the fallback to clear text communication and if operators publish a TLSA record, this also means by RFC that you must encrypt. This solves the issue with it because there's no fallback to clear text communication possible and so if something goes wrong or someone gets in the middle, you just don't send the e-mail, it should bounce. At least this is in theory then there's a problem with practical deployment as we'll see.

Next slide.

This is what happens actually. You check the TLS record and the traffic is encrypted if you can validate the certification that is shown by the receiving MTA. And so if the receiving MTA can show a certificate that matches the TLSA record, you can be sure that it's really who they say they are because also of the chain of trust that is established by the DNSSEC.

Next slide.

If you have an attacker then the certificate will not match and so you would not send the e-mail.

Next slide.

There are several operational issues and the interesting part of this project is that we actually get to meet the operators. Most of them do not really have operational feedback yet because they have never tried to use this. Most of them have never tried DNSSEC even, let alone DANE so they're still basically learning what they are. Some have so we'll see.

The feedback we get is that there's still the general perception that DNSSEC is difficult, it's complex, you'll never make it work and it takes weird cartographic stuff in the configuration, which is not really true any more. Actually, I did the test on my own e-mail server, my own personal e-mail domain and it worked very well.

The really difficult part is the DS record so again the other feedback we get is that we meet some Telcos, they say, "Okay, we'll at least start to deploy DNSSEC on our domain names," and you ping them two or three months later and they say, "No, we couldn't manage to get the DS records uploaded because we're using a registrar that doesn't support it," or "We don't really know what to do," or, "It's a different department that's taking care of the DNS." So we speak with the e-mail people and then they have to go to the network people or the DNS people and convince them that this is really useful.

So the real world feedback is that it's not really a problem with technology but it's more of a problem of organization. And even in my own personal case in which I was doing everything so I'm running my own e-mail server, my own authoritative DNS server, I got stuck for over a month because my registrar which is supporting DNS records and DNSSEC basically would not let me do it because there was a bug in the platform and the support would not know what DNSSEC is and whatever. So there's really a way to go in terms of spreading the word that this is possible and actually solving the practical problems that people get faced with when they try to do it.

Next slide.

And again—I think we already went through this—actually it's not really a matter of software, it's mostly a matter of operations.

Next slide.

Lastly, the last thing I wanted to show some statistics – there were very nice statistics – we [inaudible] still in beta so take also the data and the information with a grain of salt but what we do is we try to test domain names for all the recommendations we made in terms of e-mail security. And so part of it is whether they actually support encryption, so TLS and stuff TLS. Well, they accept the authentication on [inaudible] before starting the TLS

connection, and also whether they support DNSSEC DANE and also SPF which is outside of today's scope.

So we're still working on integrating this and we will make it public on our website, but we tried to run in preparation of this meeting asking of the top 1,000 domain names. It's by web traffic so actually it's not the top 1,000 by e-mail traffic but we took this list of big domain names and we wanted to see whether they support e-mail of course and whether they protect their e-mail servers with DNSSEC DANE and all these other technologies and this is what we found.

Next slide.

First of all, there's a significant part of them that either doesn't have MX records or they're not existing, they're not well configured so I'd say within the range of 20% or something like that. There were significant part that wouldn't validate under DNSSEC even more than those that have DNSSEC enabled, but I'm still looking into that because that looks more like a problem of compatibility or maybe in the [inaudible] user or something like that.

But apart from these, you discover that the good news is that 72.5% of these domains support encrypted e-mail but the bad news is that there's 17% percent that doesn't support any

encryption at all still in 1217 and so there's no way to encrypt the e-mail toward them.

Next slide.

And even if you go through this, you want to check which version of the TLS they're supporting which is important because as we know the older versions could be insecure. Well, we didn't even check XSL2 or 3 but, yes, people should be supporting the latest versions of the security encryption protocols. Of those who actually work and have e-mail, only less than 60% supports TLS 1.2 so the latest version and there's even a 6.5 which is stuck with TLS 1. And again, as I said, more than 20% doesn't support any kind of encryption of e-mail transport.

Next slide.

So finally we get to DNSSEC and DANE. We had 1,000 domains which are possibly the biggest at least by web traffic and so how many of these actually have DNSSEC and DANE and this is what we found. We only found 15 domains that support DNSSEC. It's how they secured their MX records with DNSSEC so it's 2% maybe and most of them are [inaudible] domains, by the way, and we just had three that have DNSSEC and also have DANE in our list.

I actually could put them here by name. One is Comcast and the other two are web.de and gmx.net which are two German providers that are part of the German project that I mentioned before. Of course there are other domain names that were not in this top 1,000 list, which we know support DANE and so on.

So you can take this. It has good news or bad news. The bad news is that the adoption is still negligible. The good news is that there are some pretty big operators such as Comcast or Web.de that are really doing it so you can go to all the others and say, “Look, if these guys are doing it, it’s possible so why aren’t you doing this?”

Next slide I think we have our contacts so I wanted to take some questions of course but the reason why I’m here is that we are really trying to broaden this project which is started sort of an internal activity by one single company but we would like to involve especially operators. And so from one point of view we organize meetings.

We had one last week in Poland which was good. We were all the [inaudible] of the country but not all the Telcos were present because it’s not in all the countries that it’s easy to get in touch with people. And so maybe by going through this kind of firms, the I-star firms, we hope to expand the reach of these and then

get full meetings with all the operators present, at least the big ones.

Also it could be interesting for—we had several ccTLD registries before and especially in European countries it would be useful to get a corporation and to involve the ccTLD registry if from one point of view they could help us in having better meetings, and also they could maybe if they want participate in explaining and pushing DNSSEC to their biggest Telcos of the country. Because I think that it's really important that this is taken as a cooperative effort by all the communities or the standards are there. It's nice to discuss the very technical details as we did but this is really the time where the community has to get serious and get deployed by everyone, at least the biggest ones, because the risk is just too big and there's a necessity, I think, to act and make this happen as soon as possible. Thank you.

JULIE HEDLUND: Thank you very much, Vittorio. I'd like to open it up for questions. Please, any questions for Vittorio?

PATRICK: Vittorio, I'm Patrick from [inaudible]. We are one of those companies who did a lot for DANE in Germany. Let me add something. You said that many people think they have problems

with DNSSEC in setting up. That's actually not the problem, you're right about that. The problem that most of the companies I've spoken to is that they have been running DNS for many years now and DNS has always been a stepchild. Of course everybody is very important so when they go DNSSEC, they're very weary they might break something in their existing infrastructure and that's something they don't want to do.

VITTORIO BERTOLA: I agree this is part of the feedback we get. There has to be a push that to win this kind of resistance because it's always easier not to do anything and pretend that the problem doesn't exist. If something bad really happens so maybe some big news in a country pops up collectively, then everyone will just rush to implement this, or maybe if you get some push from the government. But still here it's hard to convince people to act.

PATRICK: In Germany the government has adopted it. For example, [inaudible] is DNSSEC enabled and has been for many years. It's a little bit like backup and restore every [once] to [inaudible] about restoring. It's just like DNSSEC. People think it's an extra cost and they don't get anything for that.

VITTORIO BERTOLA: And by the way, Germany is the first of the class but I come from Italy. We had a meeting like this in Italy and the first problem was that we don't have the TLD signed yet in 1217. I think I was talking with all the Italian operators and we looked at each other in the face and said, "Okay, we cannot, even if we wanted."

PATRICK: I feel the pain, I know.

JULIE HEDLUND: Thank you. More questions?

UNIDENTIFIED MALE: Anyone? All those folks in the back there and you have no question at all? I have a question which was just basically what other e-mail providers have you been talking to as far as getting more people signed up to this initiative or what can people here do? Two questions, I guess, really.

VITTORIO BERTOLA: For the meetings part works like this. We pick a country, we virtually start for the biggest month so we did in France, in the U.K., in Italy, and so on and now we went to Poland and we tried to contact all the companies. Usually if their biggest Telcos, those who have millions of customers and maybe the biggest

hosting companies especially in some countries people really take their e-mail account from hosting companies or free e-mail services rather than from the ISPs, so it depends on the country.

So what we really need is helping bring everyone at the table. And of course, for example, I even tried to approach some local [inaudible] of ISOC. I've been involved with ISOC Italy for 20 years now so that could be another good point. I think we just have to share the effort and find a way to start a meaningful discussion.

Usually what's also interesting is that people tend to be somewhat nationalistic so if you say, "Look, the Germans already did all of this and no one else is doing it and in your country nothing is happening, they will say, "Okay, let's start something in our country and let's [inaudible], so that's a good card to play and also with the government.

So that may be a way to—but it's really a matter of creating awareness because people maybe they heard about DNSSEC but they didn't hear about the dangers that it's really trying to counter so they don't really know how DNSSEC and DANE can solve actual problems of security so we really need to spread the word. And if anyone wants to help, just get in touch with me.

JULIE HEDLUND: Thank you, and Wes?

WES HARDAKER: Wes Hardaker, USC. First off thank you for doing this work. I'm sort of a big fan of this technology. The one thing that we've run into a lot is making sure that people that are deploying a new certificate remember to update their DANE records. Have you implemented any test feed in the system that makes sure that nobody—the most common case is that the people that manage the SMTP don't manage the DNS so they may update the certificate and fail to update DNS? Do you have anything that checks out and watches for that in new implementation?

VITTORIO BERTOLA: No, we don't' have anything because we're still point where there are no TLSA records to be checked in most cases. But still we could implement it so it could be useful if there was a set of tools that would be shared by everyone on this. And yes, I also agree. I tried, for example, to follow the nice tutorial or nice website for deploying DANE on my own server with Let's Encrypt certificates and, for example, the Let's Encrypt client still has some real issues when working with DANE because it continues to change the key of the update. There's a number of things that could be made easier and so I think that there could be a common thought about this as well.

WES HARDAKER: All right, thank you. I will say that the company actually runs a DANE testing suite website that if you go drop your e-mail there, he'll actually notify you when you mess up. I wouldn't rely on a third-party service like that all the time without a relationship but it will actually notify you when it knows that your certificate doesn't match your DANE records.

JULIE HEDLUND: Thank you. I see another question. Go ahead.

UNIDENTIFIED MALE: Actually a comment on the Let's Encrypt issue. You can actually keep your same key – your public or private key and just regenerate the certificate. For instance the tool dehydrator does it very well because we run into the same thing – we want to keep using the same key.

VITTORIO BERTOLA: I think you have to prepare a CSL file and use that again and again but it's not that immediate and so on. It takes some time.

JULIE HEDLUND: Any further questions? Then I want to thank Vittorio for joining us and please join me in thanking him. Just to continue on, we

next have a presentation by Carsten Strotmann and this is on SMILLA, the automatic S/MIME encryption. I think it was originally going to be a demo but I think now we're focusing on doing this as a presentation. Carsten? You're hiding. You can be in the front, if you'd like.

CARSTEN STROTMANN: Oh, no, no, it's okay here. And next to me is Patrick. Patrick will actually take the first part of the slides and I'm doing the later part.

JULIE HEDLUND: I apologize. I did not realize that you were here, Patrick. That's Patrick Ben Koetter, everyone. Thank you.

PATRICK BEN KOETTER: I get the opportunity to crack a joke about talking about DANE in Denmark with all of the Danes around.

We heard about DANE in e-mail and we hard about DANE in STARTTLS protection and what it can do about that. Let Carsten and I add something new on top of that. We would like to talk about a program we've written. It's the old ITF stuff. You need ref consensus and some running code and we added the running code for a proposal that's called SMIMEA and it's all about

opportunistic S/MIME encryption in e-mail. So before I delve into that, let's first get a sense of what it's all about and why would you want to have that.

Just the other day I spoke to a technician from a larger German broadcast service and of course I do e-mail and he asked me a few things about e-mail, about how we would rebuild or build a new system, and one of the things I've been telling him was that, "Well, you work with journalists and your journalists work with informants or whistle blowers as you would like to take that and there should be some way to protect the communication because the communication in journalism probably only really works well if you have trustworthy channels and privacy." So, yes, he agreed on that and this is where it's simple is you run into a few problems that you have today.

One of the problems we have is that—oh, sorry, next slide please. No, the next slide please, sorry.

One of the problems that we have with encryption today is that it's complicated. You have two models that concur with each other—that compete with each other, sorry, and none of them is really easy to use. One of the models requires you to do some magic on the command line and you have to put out the key and people need to download it and then there needs to be some kind of trustification process besides that. It's not really useful

for instant communication if you need instant privacy. Same goes for the other standard S/MIME. It's rather complicated to put that up but then, of course, you have authorities where you can buy certificates and that makes it easier.

Next slide please.

The question is, are they really trustful? We have had a few certification authorities being abused in the last few years and having your key or having somebody else impersonate you in a S/MIME communication is probably not what you want if somebody goes and builds or steals a certificate at a certification authority.

What is it that you can do to get around those problems I mentioned? One thing is probably to gain more control about saying which certificate is a trustworthy certificate. The other probably is to speed up or get one step ahead with the encryption process. This is what the idea of S/MIME is all about.

Can I have the next slide, please?

The basic idea is to use DANE which relies on a DNSSEC enabled domain and to put out some criteria, some information that helps others to identify a few things. The first thing is there is a special record—Carsten will talk about the record later—that tells you this person you are trying to write to has and supports

encryption. The other thing is the fact that there is a record out there tells you that person actually wants encryption and a special type of encryption key that is public out there also tells you what kind of encryption a person supports. So you're not trying to use PGP while the other person only supports S/MIME or something like that.

That's the one thing you do. The other thing is you add a trustworthy channel that's a DNSSEC channel and by putting that into the DNS, you give more control to those people who actually run the DNS which usually are the people who are also people in the domain. So you've taken it away from the certification authority which might be compromised and you've put it on your own platform, of course, with all the problems you have to deal with security issues to make it as safe as possible as well.

So basically what you get is you have a mail client and a mail client is able to look ahead, find out the person you're trying to write to resides within a DNSSEC enabled domain. There is a special record and the record contains some information that your mail client can use to encrypt communication to that person instantly opportunistically the moment it finds that information. So you're one step ahead of the whole process where you need to get to ask somebody, "Excuse me, do you

understand? Do you have encryption and all that?" You get around that.

Next slide, please.

This is where Carsten takes over.

CARSTEN STROTMANN: Thank you. Next slide, please.

The SMIMEA record, it's a [cutting] of the TLSA record that we currently already use to secure our e-mail, [inaudible] and SMIMEA can be used to do end-to-end security with S/MIME certificates. The SMIMEA record can be used in multiple ways. It can store the hash of a certificate or it can store the full certificate in DNSSEC secured domain.

Our case here which is MILTER, we use the whole certificate so the whole certificate, the whole x509 certificate is stored in DNS and it's stored on a domain name which contains the hashed e-mail local code that is the part of the e-mail address that is before the @ sign.

We can use certificates here that we can buy from certification authorities but we can also use self-signed certificates. Using self-signed certificates has even a few benefits because we can

control ourselves, how long these certificates are valid and when we want to roll them.

Next slide, please.

So SMILLA. What is SMILLA? SMILLA is a MILTER and MILTER is a standard API for popular Open Source mail servers for Postfix and Sendmail and a few others, and SMILLA is actually aimed not for the private user at home but for mail providers organizations that run their own mail infrastructure.

So SMILLA intercepts all e-mail that go through the mail server and looks whether that e-mail is already encrypted and if it is not encrypted, it will then look in the DNS if the recipient of that e-mail has published an SMIMEA record containing a full x509 certificate. And if it does, it downloads from DNSSEC certificate, uses that certificate containing the public key and encrypts the e-mail with a public key and sends that on to the recipient.

Next slide.

This has two different use cases. It can be used to encrypt outbound e-mail so when it is used on the sending site, the sender's mail server will just fetch the recipient's certificate, encrypt, and then send it through the dangerous Internet to the recipient and it's received there and the recipient can then use a private key to retrieve it, or it can also be used to encrypt

inbound e-mail. So even if the e-mail is delivered completely unsecured and not encrypted, when received on the mail server site of the recipient, it can be encrypted and then stored encrypted on the hard drive.

That is a use case that can be used when the mail server is on an untrusted platform – maybe on some rented cloud server somewhere where the operator is not really the owner of the equipment so the server or the storage can just be stolen and then misused and to counter that all e-mails can be then encrypted for the recipient here.

Next, please.

Here we see how DANE with SMIMEA works and in this example both on the right side publishes the SMIMEA record in DNS. This is something where Bob probably need some support from his e-mail operator and his DNS operator. Bob stores this SMIMEA record containing his x509 certificate in DNS on the example .com authoritative DN server—next slide—and now Alice on the left side wants to send an e-mail to Bob. They have never ever exchanged certificates or keys before. They've never met, they've never certified anything.

Alice sends the e-mail completely without any changes with any mail client software to the mail server—and even Alice doesn't need to be aware that there is a SMILLA and anything involved

here—to the mail-server. The mail-server is running the SMILLA MILTER—next slide, please—and SMILLA will now look whether that e-mail is already encrypted. And when it is neither encrypted by PGP nor with S/MIME, it then—next slide—looks for the SMIMEA record in DNS.

So it goes through the DNSSEC resolver and the DNSSEC resolver goes to the authoritative server for the recipient's domain—answers coming back on the next slide—is DNSSEC validated and then given back to this SMILLA MILTER which receives and extracts the certificate from the response, encrypts the e-mail to Bob with the certificate, which is on this next slide, and then sends it out to the e-mail server of the servers used by Bob. And then on the next slide, Bob fetches the mail via his preferred mail program and can decrypt the e-mail using his private key which he has configured in his software.

Next slide.

So this is already working. The SMILLA MILTER is written in [inaudible] and it's not big, a few thousand lines of code but can be well understood. We hope it's Open Source and we have plans to merge that with the OPENPGPKEY MILTER written by Paul Wouters which does basically the same thing just for a PGP. There's an OPENPGPKEY in DNS where you can store your PGP public keys in DNS and which works basically the same. It's

completely transparent for users. The users don't need to change anything. Once that is deployed on the mail infrastructure it will automatically encrypt all the e-mails for which SMIMEA or later OPENPGPKEY stuff is in the DNS. It works inbound and outbound and we have that made Open Source with the permissive license on the find code on our github account.

So currently it's [inaudible] but we are open. If someone doesn't like [inaudible] and wants to have it in [inaudible] or anything else which is in vogue today, because it's not many lines of code, we can adopt that. Either anyone can adopt that themselves or we can help in the process of doing that.

We are interested in learning from anyone who wants to deploy this, make use of this either in production or in a test environment. Please let us know.

And the takeaways—next slide, please—the mail users care about security. We have found that with some customers who work on that to provide secure mail service and try to set themselves apart from other mail services and yes there are a larger group of users that really care about security and want to have their e-mail more secure but they fear working with all this encryption stuff and making this easier is what DANE can do. It allows for this opportunistic end-to-end encryption and maybe

it is a legal piece that we can use to make e-mail and Internet communication more secure. That's it. Questions?

JULIE HEDLUND: Thank you very much, Carsten and Patrick. I'll open it up for questions. Please go ahead. Yes, go ahead, please.

WOTH STUFFBERG: This is Woth Stuffberg, IS. What was the DNS record that you have to add to get the certificate?

CARSTEN STROTMANN: The DNS record is the SMIMEA record and the SMIMEA record is currently an Internet draft which just passed Internet Working Group last call, as far as I know, so we will probably see an RC very soon now. And also it's already supported by the newest version of most DNS software like Bind on Unbound. It can be used there and for all other software that doesn't support SMIMEA records directly. There's always a possibility to enter the SMIMEA record in unknown record format which is a standardized format that you can use to put anything in DNS even if the DNS server doesn't know about it.

So it is usable today and we are about also to write a small tool that you can use to give it your certificate and your e-mail

address and we'll spit out this SMIMEA record that you can put then in DNS because today there's no such tool and we want to make it a little bit easier and expect that to be next week or the week after available on our github account.

PAUL WOUTERS: Sorry, I haven't had many cycles to actually cooperate with you guys. I'm still glad that you're in there and still trying to merge everything, so awesome. I'm collecting all these tools in a package called Hash Slinger that collects all these generating things and so if we either can work together to get an SMIMEA command in there, that would be great.

UNIDENTIFIED MALE: Expect a merge request.

PAUL WOUTERS: Awesome. And then just one note: Me personally I once accidentally ran the OPENPGPKEY version of this on my forwarding mail server and within an hour when I checked my e-mail, I had like 200 encrypted emails and I could definitely not deal with that. So there's definitely work to be done in the client side where they preferably automatically decrypt incoming e-mail and store it in your mailbox unencrypted so that the users can actually deal with it. Because if you have 200 encrypted e-

mails in your inbox, there's nothing you can do with it and that's what I'm hoping like if [Enigmail] or other tools can do that,

CARSTEN STROTMANN: Yes, [Enigmail], there is support for that in [Enigmail] already. You can have a filter that says once I have opened an encrypted e-mail, store it unencrypted so that it can be indexed and such. That's possible but it's not by default. You have to write that filter and yes, it's an area of more work that could be done.

JULIE HEDLUND: I see Rick Lan. Go ahead Rick.

RICK LAN: Hi. Rick Lan. Great work. Really good to see this. Are you looking at any way to try to make this really end-to-end so not at the server but on the client machines? Have you though about any kind of obnoxious ways to intercept traffic say on a Windows machine so that the average Outlook user could also benefit from something like this? I'm just thinking about the masses and getting true end-to-end say you really don't trust anybody on the way through.

CARSTEN STROTMANN: It's a tempting idea but at the moment given other experience I've probably had, I would expect to fail just remembering all the antivirus tool providers who try to break up TLS sessions, things like that, in order to have a look into the mail. It's not an easy task to get it done quickly, yes?

RICK LAN: No, no, I know. Thank you. I'm definitely going to use this stuff. This is really, really fun stuff. Thank you.

UNIDENTIFIED MALE: So, Rick, just to answer that, what I was thinking of because I want the same thing is to run a mail server on local host and so you become that first hop but I would like to have that on my iPhone and I'm not sure how that will work.

RICK LAN: Yes, that would. Thanks

PATRICK BEN KOUTER: There is something else you can already do today is if you use two auto configuration tools in e-mail clients, you can provide configuration that makes them use STARTTLS on a submission path. So you go over a STARTTLS encrypted way and the

moment the mail hits the server it gets encrypted. That's one way to get the encryption.

JULIE HEDLUND: Thank you. Any more questions? I don't see any so I want to thank you both Carsten and Patrick for a very interesting presentation and please everyone join me. Our final presentation is from Dan York and this is on DNSSEC How Can I Help.

DAN YORK: So somehow we did it and we wound up hitting our schedule—here she offers me the clicker. Will I take the clicker? Will the clicker work? Sure we'll see how this works.

So we did it. We hit the end of our schedule and we actually did so a few minutes early. I'm not sure if we've ever done that before but before we do that I would just like to say can we get a round of applause for the Program Committee who did help put this together. Could we just do that? And I also want to say thank you and a round of applause for Julie and Kathy who make this all work.

The Program Committee does meet weekly every Wednesday morning for time immemorial, it seems. I've had this weekly meeting with Julie and the rest of the folks who have been part

of that. Yoshiro comes in from like midnight Japan time—is it certain? Yoshiro's here, yes, he's here. I admire his dedication for coming into this and other people who are on that.

There's a really good core group of dedicated folks who've been doing this over… now this is 10 years. I have not been doing it for 10 years but this program has been going on for 10 years so it takes a lot of work but I do want to especially highlight Julie because she's the one who puts the stuff into this matrix and gets all these different things in and helps people work with the stuff that we need to do to pull this off.

We will be putting out a call for participation shortly for the Johannesburg session that's down there. That is a little different. It's like the one we did in Helsinki where the current thinking is still that we'll merge with Tech Day and we'll do the DNSSEC Workshop in the morning part of things, right? Yes, morning and then we do morning and lunch and then we will do the afternoon. It will be Tech Day awards, other technical presentations that are not DNSSEC related typically so we're getting other things - DDoS attacks, measurements, botnets, we get all sorts of different things that come in there and other things that are part of that.

Jacques Latour who is not here from CIRA—oh, there he is. Oh, he wore the hat, man, all right. Oh, the lights and you're missing

your scarf. No plaid shirt either. How many people laughed when they saw the CIRA thing in the bag? Did you see it? All right, well, they didn't laugh, okay. Well, I laughed. If you look in your bag, if you didn't just throw out all the stuff that was in the bag but you looked at what are the pieces of—CIRA did a nice thing anyway. Kudos to them.

But Jacques is also on the Program Committee for the Tech Day so if you ever want to bring a technical presentation to another group here, really the two sessions within ICANN, the meeting here, that are technical are this day and that.

Oh, here, okay. See what I was talking about? Look at this and smile. I love that there's an organization that has a sense of humor anyway with doing things. And especially they have a little mousse in there and everything else. Okay, these are the same folks who gave out the Beaver Plush toys a few years back so kudos to CIRA for having a sense of humor.

What we'd like to end up with a little bit is just to say what can you do when you leave here if you can go away from this and do something. We asked TLD operators to do this, sign your TLDs except the records because we have some people who sign in their TLD but then they don't take records from registrars so it's kind of like awesome that you signed it, great we could check another box off but you're not actually doing anything to help

make things a little bit more secure. So we ask you to do that. Please work with your registrars.

And another note that we ask for operators is can you help us with statistics? You've seen a number of presentations here. We've talked about things like Rick Lan's site that shows statistics. We're trying to be able to get more of those so if you can help us with that.

For zone operators so people who have domains, sign your zone, work with your registrars. Again, help us in some way but really we're asking people go back, sign your domains, if you can, and don't forget the KSK roll as it's coming up October 11th.

Network operators, we ask you please turn on validation. It takes a line or so in your code. Sometimes it's on commenting something, sometimes checking a box. It can be easy. We ask people to just do that. Let's watch the APNIC percentage of validation increase over time. We'd really like to see that so, if you can, go back there and do that.

We ask everyone to please use DNSSEC, share your lessons. Like I said, we will have a call for participation for this next event. If you're going to be in Johannesburg or if you know people who are for that policy forum and you'd like to present on stuff that you're doing, we're always interested in different ideas. We'll do another regional panel so if you know people from the region

there, obviously Africa, who might want to present about what they're doing with DNSSEC, we'd love to hear from them.

We're also looking for people who are doing new demos. We've heard stuff about—now with e-mail with a couple of different pieces here. We've had other e-mail presentations in the past, we've had people doing some things with other different tools, new tools they were demoing, new sites hat they may come up with. We had Rick doing a soft HSM one time, we had other different kinds of things that people have done so we're always looking for different kinds of presentations really wanting to focus on how are people using DNSSEC and DANE in ways that make sense.

So with that I want to end by just thanking—oh, Christian, you're right, man, sorry. We need his new logo on there. There's a really nice shiny, colored logo on his website. We're sorry, Christian. We'll get it up there on the next one but we want to thank Afilias, CIRA and SIDN for the support they gave. If you see Christian around, he was sitting over here, white shirt, thank him. Thank Jim Galvin if you see him. Thank Jacques. We can all thank Jacque. Thank you, Jacques. There why you had that lunch that you did have earlier today.

And I think we said this again, SSAC and Deploy 360 program and that's it. We'll point you to some sites out there, the Internet site

at org/deploy360, a program we have there, DNSSEC tools. It has a number of the different tools that are out there and the DNSSEC deployment that org site has more historical info that is there.

So with that—oh, one last thing, hey, we need to update that slide. I know you sent them to me and I obviously missed that when I did that one.

UNIDENTIFIED FEMALE: We can all see you in Copenhagen.

DAN YORK: Yes, you're right. So ignoring that last line, I will say that if you've been interested in some of the topics that have come up, we do have another effort that keeps many of us connected between these events. Every month on the first Thursday of the month we have a conference call that about typically a dozen of us participate in or more. It ranges but anybody is welcome to attend.

We talk about what people are doing, the new steps, we watch Rick wander around California getting coffee because it's that time of the morning and we do get to talk about what other people are doing and what steps they're doing to implement new things.

So you can just join this mailing list. It's up here called DNSSEC-coord as in coordination and we do have these calls and we'd be glad to have people participate. It is a nice way to learn what other folks are doing. We've had many people learn and we find, oh, K. C. [Devaccio] is doing this testing thing and Wes Hardaker says oh, that would be interesting for what we're going to do over here, or different people talk about other different programs that they're doing and it's a great way to share and keep this building as we go from session to session and moving on from there.

With that I think we're done, so thank you all and we will see you in Johannesburg, Jo-Burg.

JULIE HEDLUND: Thank you, Dan. Yes, for all your leadership and for doing basically all of the moderating today, pretty much.

DAN YORK: Yes, and next time if there's somebody else who'd like to help with moderation, make yourself known because I don't need to be the one doing this all the time. Thank you all. We also have to thank Irwin right here. If you get a chance thank Irwin for the DK, the implementers gathering last night and for local support. Thank you.

[END OF TRANSCRIPTION]