



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #008
(Transcription services provided by [PWOP Productions](#))



Brian Komar Talks PKIs
April 27, 2007



[Music Playing]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio - The weekly Internet talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing Show #8, with guest Brian Komar, recorded Thursday May 10th, 2007. RunAs Radio is produced each week by Pwop Productions - Offering professional media and Podcasting services, online at pwop.com.

Richard Campbell: Hey, this is Richard Campbell and you are listening to RunAs Radio and with me, my co-host, Greg Hughes.

Greg Hughes: Hello everybody, hi Richard!

Richard Campbell: How are you doing man?

Greg Hughes: Doing pretty well, how about yourself?

Richard Campbell: Well, we're all West Coast, so, it can't be anything but good this time of year.

Greg Hughes: That's right, and this time of year is the time of the year to be where I am at in Portland, Oregon, as opposed to the other time of the year.

Richard Campbell: Which would be winter.

Greg Hughes: Right, we have two seasons here, they say pretty much its rain and construction and everybody has their favorite.

Richard Campbell: I got an email.

Greg Hughes: Cool!

Richard Campbell: Let me read it to you, "Hi guys, thanks for the great new podcast, I will be paying attention to this one. I am in a small office, where we are very much data driven, and we have lots of big important data files. We have 500 mega byte access files, SPSS files and about 40 gigs of SQL server databases that all need to be backed up."

Greg Hughes: 500 meg access files.

Richard Campbell: That scares me.

Greg Hughes: It happens though.

Richard Campbell: It's true, and it goes on to say, "Not large by the standards, you might be talking about but large enough to make backups painful."

Greg Hughes: It does.

Richard Campbell: "I was interested in the comments about Disk-based Backup versus Tape Backup." We are discussing out options right now, and of course this is one of the questions, we have to answer. "Like you, I think the time for disk based backup has finally come but I am having trouble finding material that backs me up". No pun intended.

Greg Hughes: No pun intended, I am assuring you.

Richard Campbell: "Do any of you have any references that outline the benefits of disk versus tape or the benefits of tape versus disk. Also could you find examples of companies that have successfully made the switch to disk-based backup? Backup is not the best area to be an early adopter. So, I need to show that disk-based backup is beyond the early adopter stage, I am looking for you to back-up your comments about backup. Looking forward to more IT podcasts, I think, you've found a neglected niche, if that niche can be huge. Good luck, Scott Stonehouse."

Greg Hughes: Yeah, and, of course, IT professionals love to explain how neglected they are, that's what we do, right? So, just kidding.

Richard Campbell: I know of course the IT credo change is good, you go first...

Greg Hughes: That's right, exactly.

Richard Campbell: Who wants to be -- find out that backups didn't work?

Greg Hughes: And you know actually, IT organizations that I have run and worked in, have always been a little beyond leading edge, quite often bleeding edge in some areas; backup is an area that's always been really painful for people, but actually we have done and have made the move to some disk-based backup, and we have some background in that area and it might be something that is worth touching on for a show.

Richard Campbell: Do you think we could do a whole show just on disk-based backup?

Greg Hughes: Well, you know, I do. It might be interesting to find out if what our listeners think.

Richard Campbell: Yeah, do you want to hear a show on disk-based backup send us an email info@runasradio.com.

Greg Hughes: Yeah, we could do that. I imagine that I could probably find. I know a number of



people who have expertise in that area, we could probably find somebody to come on and provide some real solid backup information, so yeah, let us know.

Richard Campbell: Great! Alright, let's introduce Brian Komar. Brian Komar is the President of IdentIT Inc. and a security consultant specializing in public key infrastructure and identity lifecycle management engagements. He is the author of *'Microsoft Windows Server 2003 PKI and Certificate Security'*, published by Microsoft Press and co-author of the *'Windows Security Resource Kit'* with Ben Smith. He is also been a Microsoft MVP in security for I think the past three years. Is that right Brian?

Brian Komar: Yeah, that is correct.

Richard Campbell: And welcome, thanks for coming on the show.

Brian Komar: Thanks for having me.

Greg Hughes: It's good to talk to you Brian.

Richard Campbell: Alright, I have got two security guys on the show today, I know I am outnumbered.

Greg Hughes: Look out!

Richard Campbell: So, we were talking about EV Certificates. So, and your comment here is great, does anybody notice the green bar anyway. Mostly we notice when Certs are bad.

(00:05:07)

Brian Komar: Right, Microsoft has gone a long way with IE7 and we are starting to see this as well with Firefox. The idea of trying to give better indications when there is a phishing site, so that you know you are connecting to a bad thing. The whole idea is that a green bar means, it is good, it has gotten these new extended validation or an enhanced validation certificate, and a red bar means bad.

Richard Campbell: Right and EV Certificates meaning Extended Validation Certificates.

Brian Komar: Right, the idea of the Extended Validation is that they are going to limit who first of all can get the Extended Validation Certificates. You must be a corporate identity, and you must have - I think it's a hundred thousand dollars an annual sales each year to even qualify for an EV Cert and then they are really supposed to take measures to ensure that the person requesting the Cert is a true

representative of the organization requesting the certificates.

Greg Hughes: Right, and then it is not some bad guy out there trying to get a certificate for my company in order to commit fraud for example.

Brian Komar: Yeah, like for example somebody getting a Code Signing Certificate for Microsoft, like that would ever happen.

Richard Campbell: Oh, there is a little sarcasm today...

Brian Komar: Yeah, that happened three years ago, in fact.

Richard Campbell: Really?

Greg Hughes: Yes, it did.

Brian Komar: If you actually look, there is a non trusted certificate store and that certificate is one of the certificates in there.

Richard Campbell: Yeah, don't trust his Cert and it's an interesting problem. I think we are in a new place these days, where it's not that big a deal to get a certificate of some kind. So, now we are really talking about the leg-work necessary to really have an identity company, identify someone before they give them the certificate.

Brian Komar: Well, this is my one problem with the EV Cert is that what they are promising to do, is what they were suppose to do in the first place and they charge you a premium for it.

Richard Campbell: Right.

Greg Hughes: Right.

Brian Komar: And I think that's one of the major issues that some companies are facing today when they are looking at the decision to do EV Cert. One of the big things we've noticed is that, people aren't noticing the green bar. They have done a really good job with the red bar now. You know, no more just a little dialogue popping up and saying, this site may be bad, do you want to continue and the default option was, yes.

Now, it's, this is bad, this site doesn't match, the certificate is revoked, can't determine the status of it and then says, you should close this website recommended and that's the default option, if somebody were just to click 'okay' at that point. I think they have done a really good job on that end. The green bar though, it's kind of a two-fold institute for me, one is we have got to advertise to people that the green bar means it's a god site, first of all.



For example, the first commercial site that's using it today is paypal.com and I wonder how many of the listeners of this show actually realized or saw that there was a green bar when they went to PayPal and got that warm and fuzzy feeling.

Richard Campbell: Yeah, did they actually feel good about it, do they even know that, that was a good thing that happened.

Brian Komar: Did they even notice that the bar was green? We actually sent one of our employees to the website and asked them afterwards that if they noticed that the bar was green and they had not even noticed.

Greg Hughes: So, I think I mean, we are talking about Web Server Certificates and the interaction with the web browser, before EV Certificates, you know the general instruction and even it was a weak instruction and could have some real problems associated with it, was look for the little gold lock.

Richard Campbell: Right.

Brian Komar: yeah, and I took it further, I said, click on the lock and look at the company that issued the certificates and ultimately at the root, do you get a warm and fuzzy feeling about that company as well?

Greg Hughes: Not to mention, look at the details of the Certificate and make sure that there is actually any encryption at all taking place because it is possible to get an SSL Certificate and not have encryption.

Brian Komar: Yeah, they could say that there is no encryption on this site at that point as well, so you know and here is one of the other things that's happening though is, if we make a big push that green is good and let's say convince the employees of our companies, only put information when the website is green.

Greg Hughes: Right.

Brian Komar: Well, a lot of companies today are deploying internal PKI's for internal use. So, for their intranets, for Internal Code Signing, EFS, 802.1x Wireless Networks, etcetera. Well the thing is those will never be green because to be an EV Cert distributor, you have to put a specific object identifier into the certificate with a new extension, and then you have to include in the list of EV Cert providers.

So, if you go down this path of convincing everybody, this is really good, this is really good,

but when you go to your human resources website, white is okay too.

Richard Campbell: Yeah, an interesting problem that if the internal stuff is not going to have this, it's only going to be external, so now you have to give them awareness of where you are looking?

(00:10:05)

Brian Komar: Yeah, it almost becomes now that people will have to start looking more and more at the bottom bar of the browser saying, what zone am I in for security, what colors is the bar? It is putting a lot of onus again on the user. I think it is a good intentioned idea. The idea of let's make sure that we are not selling certificates to the incorrect person. But all it's going to take is one company to screw up, that's doing this issue and if we hear of one case of somebody is being told, we are sorry about the over billing we did, here we will give you the EV Certs instead and they didn't actually do the full check of what they are supposed to do, it just totally devalues the whole lot of EV Certs.

Greg Hughes: Yeah, that would be a real problem.

Richard Campbell: So, who's handing out the authority to give out EV Certs in the first place, is that can ICANN function?

Brian Komar: It's a combination; there is a committee that's been put together, and I am not sure exactly where their jurisdiction comes from but you have got VeriSign, you've got Certitrust, CyberTrust is in there, GeoTrust. So, there are several companies that are taking part in this. And, in fact IE has actually jumped the gun, because they still have not come up with a formalized solution yet.

Greg Hughes: Right.

Richard Campbell: So, IE is turning green on what it thinks an EV Cert is going to be.

Brian Komar: Well, it's the latest draft of the spec, you know, it will not be hard to change the behavior, if the behavior changes in the spec it would be an IE patch which, we are all unfortunately familiar with.

Richard Campbell: Getting them every Tuesday.

Brian Komar: Well hopefully, the first Tuesday of every month.

Greg Hughes: And I think it's reasonable to say that the Firefox team that clan is also working on



and doesn't tend to deploy support for the EV Certs in the near future as well.

Brian Komar: Yeah, I think as I said, I think in general, the intent is great but my whole thing comes down to it, weren't these SSL companies supposed to be doing this in the first place.

Richard Campbell: Yeah, I remember a day in the 90's where I was looking to getting an SSL Cert and I needed a notary public and all those sorts of things done to be able to get the Cert at all. Now, this all seems to have fallen by the wayside.

Brian Komar: Yeah, you know, it also comes down to policies and that's a big part of any PKI deployment is the Certification Practice Statement and the Certificate Policy, where you are saying what measures -- you know the Certificate Policy, the definition is, what measures did you take to identify the subject of the certificate, before you issued them a certificate, so I can base an assurance level on that certificate.

Greg Hughes: So, let's make an assumption and it may be a bit of an optimistic assumption but let's assume that the certificate issuers do follow the rules and they do the proper validation. If we accept that as a 'given' then where do we stand today with EV Certs versus where we were before them?

Brian Komar: Well, I think people will have a more comfortable feeling as to when they go to an SSL website, and they see it is green, they will feel much better about doing commerce on the Internet.

Richard Campbell: I know what the problem is here; the problem is that most people don't feel bad about it right now.

Greg Hughes: That's a pretty good point.

Brian Komar: I thought, you were going to see most people are colorblind.

Richard Campbell: Well then, that would be, why it had to be green? Isn't that the one they are not going to be able to see?

Brian Komar: Green, red the usual, you know, green good, red bad.

Greg Hughes: Well, there is probably a reasonable question which is, do I really need to be as well-trained about green, or should I be well trained on red?

Brian Komar: I think, that's even more important -- when it's an obvious attempt where something is wrong, I think you hit around the nose Greg, as we have to have more attention to red, name does not match, the certificate is revoked, not within its validity period. In fact, I wrote a whole whitepaper on Revocation and Status Checking for Microsoft and it's a major area for a lot of people to understand, but I think for the end user out there, you know, for our Moms on the Internet, I think this is the real important thing is that red is bad, to close the window and I think it's great that they are making the default abandon.

Richard Campbell: Yeah, walk away.

Brian Komar: Walk away.

Greg Hughes: I agree, I think the improvement is definitely in that red flag zone and that the EV Certs -- the value that you get just in that one area, is pretty darn good.

Richard Campbell: The question is how far away are we from being able to adjust the policy on our Mom's computer, so that no site that doesn't have a green SSL is going to work.

(00:14:53)

Brian Komar: Well, with IE today, that's pretty much been the case; if you are running on Vista, Windows Vista with IE7, I'm actually answering a few questions on the public news groups about this because people are having problems with clock sync for example and their dates are wrong on their computers and they are getting issues when they are connecting to these websites, because revocation list isn't within the current timeframe. So, they are getting the red bar when they shouldn't be.

Richard Campbell: Because their machine is defaulting to 2000.

Brian Komar: Oh! It is something like that yeah. So, what they are getting under the hood is the certificate is not yet valid.

Greg Hughes: I think one of the other important points about EV Certificates and you mentioned earlier, what kinds of companies can get them now. And the average small business or non-corporate business doesn't really have that option available and so, where a lot of high-profile maybe first wave big websites are able to deploy EV Certs, it's not something that is extended to every business today.

Brian Komar: No, it really was excluding individuals for purchase of the EV Certs.



Richard Campbell: Is that a good idea, shouldn't anybody be able to buy this, if they can produce the proof of relevance and of appropriateness?

Brian Komar: I think they wanted for the first draft of this, for the first round of it to really limit it to corporations. I am just looking up on the definitions of it, and really the big part was that it is intended for corporations initially.

Greg Hughes: Typically, corporations that have a Duns and Bradstreet numbers, sort of, seems to be the -- in other words large enough to where they have a high enough profile that you can actually do some validation and put some meat on the bone.

Brian Komar: Right, so it's not just a company setup in the middle of the night and getting a Cert and doing business and then shutting down a week later.

Richard Campbell: Yeah, but I mean a D&B I immediately think, they have got to be a publicly traded company.

Greg Hughes: And, I think quite often that, that is the case. You know, the question is, is that the right thing to do? I think the vast majority of big businesses and this is just my opinion are eligible to get the EV Certs and I guess, the real question, is if you can do it for them now, isn't it time to do it, or do we need to wait and put a lot of complicated bureaucratic infrastructure in place and wait to even offer this, until we can extend it to the smaller business and I think the answer ultimately was, no. There is a real need right now, with some very large high-profile corporate entities that are being defrauded or that are being fraudulently represented. There is a real need to get this capability out there now, and then in a second phase and maybe a third phase, to roll that out and to make it available to some of the smaller companies and individuals.

Brian Komar: Yeah, and I think it will actually take much more legwork to validate a smaller company. It's going to be much more of a process for the certificate providers.

Greg Hughes: Yeah and probably a much more manual process.

Richard Campbell: Well then like you pointed out, the first -- one of the very first sites that EV Certs in places is PayPal which is one of the most phished sites in the world.

Brian Komar: And I think, that's why they really felt they had to go with the EV Certs. If you don't see a green bar when you are connecting to PayPal --

Richard Campbell: You know it's a fake.

Brian Komar: Yeah.

Greg Hughes: Absolutely or if you see a red bar when you think you are connecting to PayPal or to your bank or credit union or wherever it is, then certainly that red bar and the pop up that says, hey we don't think you really want to do this is a pretty powerful deterrent.

Brian Komar: I think another thing too that browsers are doing is they are blocking those windows that don't show title URL bars anymore, they all show URL bars. So, if somebody is trying to do something fancy by doing a pop up window and trying to hide the bar, so you don't know where to they are going, you do know, with IE7 you are getting that always for the part of the experience because I think it is important too.

Richard Campbell: And I just double-checked Amazon.com and they are not a green bar.

Brian Komar: Actually I've talked to one of the people over at Amazon and they doubt that they will be.

Richard Campbell: Interesting choice.

Brian Komar: And they just feel that the cost addition for EV Certs would be cost prohibitive to their customer.

Richard Campbell: How expensive are we talking here?

Brian Komar: What was the current pricing on them, it's ranging by providers, but they are at least double in some cases.

Richard Campbell: So double being...

Brian Komar: The current SSL price.

Richard Campbell: How much is a current SSL?

Brian Komar: From VeriSign it could be \$250 per year.

Richard Campbell: Oh come' on,

Brian Komar: With some it could be \$500.

Richard Campbell: How do you justify that? You know, you are talking about a company that's got at least a certain level of sales and they are going to have problem with a \$1000 or \$2000 a year.

Brian Komar: No not for a single Cert, they are talking thousands of certificates.



Richard Campbell: Right every machine with its own Cert.

(00:19:56)

Brian Komar: This is where it starts to come in. We are not talking about companies wanting to buy one certificate, here is one certificate I don't think these big companies would have an issue.

Greg Hughes: I think again this is an area where this will happen in phases and as the EV Certs becomes even more mainstream certainly they are available today in a standard, or a proposed standard which will likely be ratified as it sets but as they become more mainstream and more adopted - as it is with any new product, if you will, that the rules and the prices and the availability does tend to change.

Brian Komar: Yeah, I think, economies of scale will kick in the next couple of years on them.

Greg Hughes: You mentioned earlier, you were talking about certificates and validation on the intranet; that kind of raises for me the question of maybe like a PKI Infrastructure inside of companies. What can you tell us about that, is that an important thing or what you see the value of that being?

Brian Komar: Well, I see a lot of value and that's what our primary consulting businesses is with our company.

Greg Hughes: Here is you go, because historically it's been pretty difficult for companies to do it in a way, that A allows them to really leverage it, and B provides a level of usability that isn't cost prohibitive.

Brian Komar: Exactly, I think what's happened previously is that a lot of the PKI solutions out there were very, very cost prohibitive to implement. Our company specializes in deploying the Microsoft PKI and with the release of Windows Server 2003 a really good version of certificate services is now included in your license of Windows Server 2003. And we have seen more and more applications that are driving companies to implement internal PKI's. We actually call it the killer app, whatever that application may be. Many of our customers this has been 802.1x Wireless Authentication. They put in wireless networks and they are really concerned about the attack factor of the guy in the parking lot with the Pringles Can connecting to their network.

So, what we have found is for a lot of these internal used application, it is a really, really,

good solution to deploy an internal PKI, for example for wireless if we deploy an internal PKI we can say that the certificates must be for client authentication, but they must chain to our internal root CA, maybe even we'll put a Custom Object Identifier into the certificates and say, the certificate must include this object identifier.

Greg Hughes: Sure.

Brian Komar: In this way, if somebody buys a certificate from VeriSign, from Thawte, from GeoTrust etcetera, they are not going to be including our trust realm for our internal applications. We can designate which root we want to trust.

Greg Hughes: Right, the only way that I can access and utilize this wireless network is if I have Machine Certificate and an Individual Certificate which map against and maybe allow me a certain level, if any, access to a wireless network.

Brian Komar: Exactly, and then there are other applications like this too that we would want to go to internal root CA's for example, encrypting file system. If we want to start doing key archive on recovering and managing the certificates internally. EFS is another great example, smartcard log on, we are moving towards 2-factor authentication, I want those issued by CA's that are only trusted within my organization.

Now, there are applications, of course, that we do want maybe want global acceptance of, for example Server Authentication Certificates, the Web Server Certs, Code Signing Certificate. If we are developing any code that we want to sell to the public. The dangerous one, because nobody understands how they work, S/MIME Email Certificate, I always joke with it, you know, an S/MIME Signing Certificate, easiest certificate in the world to deploy, we can buy them from a commercial provider, so everybody recognizes it, you can sign your email, and everybody can validate your signature. But, too often people think of the encryption certificate and they think, "Oh, I will get an encryption email certificate and I can send encrypted email to anyone in the world." But they've got it backwards.

Greg Hughes: Exactly.

Brian Komar: All an encrypted email certificates means, is maybe just maybe you might be able to receive an encrypted email, if somebody can get your certificate to do so. That's all it means.

Richard Campbell: Yeah, that's not what it was intended for.



Brian Komar: Yeah, you know, and that's the thing like how are you going to do it as a company, are you going to stand up an LDAP directory and the extranet that will do this. Are you going to have all of your users send signed emails that include the Signing and Encryption Certificate to their targets? This is a big, big issue for S/MIME.

Greg Hughes: So, it is a big issue and it's a big issue for many, many companies and it's becoming more and more so, and this really has been growing in size over time. So, what's the answer? What is the answer to email security and I ask that question a little bit tongue-in-cheek, because I mean email is just really fairly blatantly an insecure medium for communication. So, how do we solve this problem?

Brian Komar: Carry your pigeons.

Greg Hughes: So, we can go back to real-time.

Brian Komar: No.

Richard Campbell: Mail is terribly broken.

Brian Komar: A lot of companies -- what they have been looking at is gateway solutions, if they know that we need to encrypt email -- intelligent gateways. So, if need to send encrypted email from company A to company B, we can do gateway-to-gateway encryption, to encrypt it as it is going across the public network and we can set up rules that will take place at our gateway, that will identify whether a signature is applied, whether encryption is applied and then what you are doing is you are encrypting it to get it to that gateway. If you are really looking at pure control systems in many ways rights management services are probably a better solution because if you think of it with secure email, all you are doing is encrypting it to get it to that target email inbox. There is no stopping them from decrypting the message and forwarding it to the public at that point.

(00:26:10)

Greg Hughes: Sure.

Richard Campbell: Yeah, I guess we are talking two different issues here, one is moving sensitive information via email and the other is effective identification of email sender and receiver.

Greg Hughes: I think we are also talking about the safe and appropriate storage of information that may arrive in email.

Brian Komar: Yeah, it really comes down to -- the way we approach it at many companies is we ask them what is their data security policies?

Greg Hughes: How many of those companies say, "What?"

Brian Komar: Over half. To be really honest, at many times that's where we're starting the engagement. You are looking at things like, what are your classes of data, because if we can come up with a classification of data, then we can say, "Okay, how are you going to protect that data, that creation and store in transit at termination?" And then you can start coming up with solutions, but the idea is write a policy that is not technology specific, so that if technology changes, you apply different technology, but you are still following the intent of the policy.

Greg Hughes: I think quite often -- little sidebar -- but when you speak to companies that put their username and password and their highly sensitive information on the same classification or security classification level as their toilet paper roll replacement policy, that's not very defensible when it comes time to go to court and to explain why it is that what this person did was really, really wrong.

Brian Komar: This is why many times we like working with Military organizations or Defense contractors.

Richard Campbell: They get security in a different level.

Brian Komar: And they got policies.

Richard Campbell: Right, serious about it.

Brian Komar: You ask about a policy, they will throw reams of policies at you.

Greg Hughes: So, what happens when you're dealing with more than one company? Let's say I have partners and I have customers out there, and there is more and more pressure on IT departments to enable an organization to better collaborate and interoperate with partners and customers, but the security implications of that are potentially pretty huge. What are some of the options that are available? We're talking about PKI, we are talking about certificates and what not, so in that general area, what's available to help me do a good job of solving that problem?

Brian Komar: Well, I just did sessions at the TechEX conferences for print and publishing where we talked about interoperability and one of my sessions was on this exact topic. What you've got really are four different solutions that are

available, and the solution that your company will select is really based on cost and requirement, but the first solution is simply buy certificates from a commercial provider. So, if you have a small group of people and you need those certificates to be trusted globally, just buying certificates for those purposes, whether it be S/MIME, Server authentication, code signing and buy them from a commercial provider such as GeoTrust, VeriSign, CyberTrust.

The big thing you look at there, their big promotion is, we are covered – we have 99.5% of the browser market. So, you are looking at that point X, how much do you need for your company? But when you start getting into large number of certificates, now you've got to revisit that, because it becomes cost prohibitive, so there's a couple of solutions out there. Many of the companies now have an offering that we like to title as root-signing. What they would do is they will sell you a subordinate CA certificate limited for the purposes you are buying, so they might limit it for client and server authentication and email.

Greg Hughes: They don't tend to put much of a limit on the price by the way.

Brian Komar: The limit actually – the companies I've worked with have done it to achieve huge cost savings when they look at the numbers, because what they're looking at is rather than paying let's say \$25 per certificate for 2000 users, they end up getting about 50% of the cost. So, they can achieve pretty good savings on these, and when these companies do these root signing offerings, what you get to choose from is, are you doing server certificate, user certificate or some combination?

Now, the catch is, when you want to do root signing, you now have to follow their certificate policies and certification practice state. So, they will define how often you need to be audited, how often you need to backup, how often do you need to publish replication information. Does your CA require a hardware security module to protect the CA's private key and what fixed level do you need? But for a lot of our companies, they like this solution, because if they are using let's say a Microsoft PKI, and they are taking advantage of auto enrollment, or maybe a registration authority such as the New Identity Life Cycle Manager 2007, they are able to do the same things they are doing, but they have a certificate that now chains to a commercial root.

A great example of this, Microsoft Corporation, if you look at any of their SSL websites, they're actually issued by internal CAs that chain to the CyberTrust root CA, the GTE CyberTrust root

CA. So, they have found a great savings in doing this, they felt that they needed the global recognition of their certificate, but they wanted to have local management of their certificate. The one big role, you can't become a certificate provider, you need to be doing this for your own company, you can't be issuing other name spaces.

Now, a third option, and this is a real quick and dirty one, but if you need to trust between another company, and you both have internal PKIs, you can just exchange root CA certificate, and add the other company's root CA to your trusted root store, and then all your clients will recognize certificates issued by your customer's PKI.

Greg Hughes: Now for people that aren't familiar with this, are there any security implications with me providing it to my partner and then putting it on their root store?

Brian Komar: Well, there are no implications to you, but there are big implications to me to take your root certificate and put it into my company's trusted root store, because now I trust every certificate your company issues.

Richard Campbell: That's a pretty high level of trust between a couple of companies.

Brian Komar: Extreme, right? So, that means if you – let's say we only did it for client and server authentication, but you have Joe Evil working, and he writes the best rootkit ever and signs it with a code signing certificate from your CA hierarchy. My users will recognize that signature and say, "It's okay." So, that's my one problem with just doing it, yes it's quick and dirty, but it's probably not a real feasible solution.

Greg Hughes: So, in some limited circumstances, maybe company A acquires company B and they need to be able to trust each other's authorities, then you have that capability, but that's a situation where the trust is probably already established very high.

Brian Komar: Yeah, acquisitions and mergers, they can work. Now, there is an option to this that can work called cross certification. Now, with cross certification, what I can do is I can issue what's called a cross CA certificate from my company's PKI to a specific CA in your company's PKI, and in there I can define restrictions based on four different attributes of the certificate. One, I can say, "I'm only going to trust, what's the path length?" In other words, the basic constraint of, do I trust just the CA I issued this to? Do I trust the CA I issued it to, and only



direct subordinates? Or maybe two tiers below, I can put it as path length equals some number.

If I say zero, I only trust that CA, if I say path length equals one, I trust that CA and only its direct subordinates. So, that's one part, so I can really limit it, like if I come to your company and I do a physical audit on this one CA, I can say, "Yes, I trust this CA. I will only trust certificates issued by it."

Richard Campbell: You are giving a level of granularity for the control.

Brian Komar: Yeah, exactly. Because I don't know if you have an office in Malibu, maybe I don't trust the way they manage their data center, now the second thing is, I can put in name constraints. So, I can put in both includes and excludes. So, I can say I only trust it for your name space for these name formats. So, if it's going to be for server, I'll only put your DNS format, that I am going to recognize. But I can also put in email formats, UPN formats, distinguished named formats etc. Even more importantly, I can put excluded ranges, and that's my favorite one to do, because I am going to say, "You know what, I am going to trust you, but I am going to exclude all my company's named formats. So, you can't issue a certificate for identit.ca at all, because that's my company's domain, you shouldn't be issuing certs to my users or my servers."

Now, the third one really keys in here, we can put in application policies. So, we can say, just like they do on root signing, we can say I only trust this for client authentication and server authentication. So, to that, Joe Evil does his code signing certificate, when it comes across, it's going to be, 'Sorry, this isn't trusted for this purpose.'

Greg Hughes: Got you.

Brian Komar: And then the last one, which gets real interesting is, we can now define certificate policies on each side and map them, transform them so we recognize them. So, we could say, my company has a certificate policy called managers, and to get a certificate with this policy, you must be a manager, you must be bonded, you must have shown federal photo ID to get this certificate. You've got a policy called Executives, that pretty much maps directly to that, we can take the object identifiers that represent these two certificate policies and actually map them and say, "My policy equals your policy." These restrictions will actually go into the cross CA certificate that I issue to your company, and now when we see your certificate, they will chain

actually to my root CA, but they are restricted by my cross CA certificate.

Greg Hughes: Now I am hearing a lot of different terminology that sounds very active directory-ish to me.

Brian Komar: It sounds active directory, but it's actually not directory based at all. If anything, it's really X509 based, it's all defined in RFC3280.

Greg Hughes: So, I can do all of these things and really be agnostic to the fact whether or not I have an active directory in place,

Brian Komar: It doesn't matter at all, you can do – in fact we have done a hybrid version of cross certification for several defense contractors in the US. They have setup what's called a Bridge CA, and a bridge is a CA that sits onto itself and participants will cross certify with the bridge, and then anybody who shares membership in that bridge, will trust other companies working in that bridge. Well, this specific bridge is called Certipack, and it was setup by the defense contractors, so that they could trust each other for secure email, for client and server authentication, and it actually cross certifies with another bridge called the U.S. Federal Bridge, which the US department of Defense hooks into.

So, they are now able to actually sign contracts and send them to the DOD and they recognize using internal certificates.

Greg Hughes: That's pretty darn cool.

Brian Komar: What's really the best part about it? Agnostic on platform, it does not matter what PKI you are using, this is not a Microsoft solution, this is RFC compliant, PKIX compliant solution. And if you are interested, there is a whole white paper on it on the Microsoft website that myself and Dave Cross wrote.

Richard Campbell: It does sound like we are at a new level now in using PKIs between organizations.

Brian Komar: It's starting to. These are options that – we wrote about this three years ago, and we are starting to see it now come into provision as more and more applications are becoming dependant on certificates. If there is anything to the listeners to warn about it, if you see an application saying, 'You need certificate,' if you see the line that says, 'Step 1, setup a CA,' please disregard that step and think about setting up a PKI for your application. The infrastructure that deploys certificates for all applications in your companies. The biggest mistake I think – and we talked about this earlier, why did PKIs



fail? I really feel it's because companies setup pockets of PKI. We have a Cisco VPN-3000, but setup a CA for it. Oh, we have Exchange 2000 with Key Management Server, let's setup another CA for this.

Richard Campbell: No central management of that is the issue.

Brian Komar: Exactly, and there is no trust, it's just little pockets of PKI within your own company. How are you going to do trust between companies when you can't even get it right within your own company?

Richard Campbell: Absolutely. Well, Brian I think we are about out of time, and I feel like we are just getting into this now, there is a lot of places to go.

Greg Hughes: It's definitely been a fascinating discussion.

Brian Komar: One area for the viewers to go, Microsoft had some great white papers on PKI at www.microsoft.com/pki and a great reference for finding a lot of the whitepapers we have discussed today during the session.

Greg Hughes: Richard, I think I know a lot of questions have popped up in my mind, and I can only imagine the questions that are coming up in the minds of the people that are listening. So, just a reminder, feel free to send questions, we can always drill down and hopefully ask our guest to come back some time.

Richard Campbell: Sure Brian, we may bring you back for a question and answers show with all the email we got.

Brian Komar: That would be perfect, and if anybody does have any questions specific to PKI, please feel free to send them to me at brian.komar@identit.ca

Richard Campbell: And you can always email us at info@runasradio.com

Greg Hughes: And we'll read your emails on the air.

Richard Campbell: Thanks very much Brian.

Brian Komar: Thank you.

Richard Campbell: And we will talk to you next week on RunAs Radio.