



RUNAS RADIO



<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 #003
(Transcription services provided by [PWOP Productions](#))



**Dana Epp talks CardSpace on the Client-Side
April 22, 2007**



Dana Epp talks CardSpace on the Client-Side April 22, 2007

[Music Playing]

Richard Campbell: Thank you, thank you very much and you are listening to RunAs Radio. This is Richard Campbell, up here in Vancouver, British Columbia with my co-host Greg Hughes.

Greg Hughes: Hey Richard, How are you doing?

Richard Campbell: I'm good, How's Portland?

Greg Hughes: It's just fine. Actually today, rare sight of sights, the sun is out and there's clouds in the sky, but the sun is actually hitting the ground.

Richard Campbell: And you've been running all over the country too. What, just back from Columbus?

Greg Hughes: Columbus, Ohio. I've been spending a lot of time, crossing back and forth across the country and that makes for an interesting schedule, but it's really a – a pretty big part of my job is getting out and seeing a lot of different people.

Richard Campbell: Well, and you're in the banking industry, you got to talk to banks. What else is there in Columbus except banks?

Greg Hughes: There's a lot of great stuff in Columbus, don't put me on the spot. There's banks, there's certainly banks. The one thing I really appreciated about Columbus and my visit there is they're really terrific people. It's always a nice town, and every time I go there, I always appreciate the – some of the things to do and it's really quite a bustling town with a lot of really nice places.

Richard Campbell: Until football games are on, you've got to go to the football game. There's nothing else going on when there's football.

Greg Hughes: That's what pretty much everybody tells me.

Richard Campbell: Alright well, we've finally got some technical glitches straightened out, the website is looking better, and we're on the banners properly for RunAs now, and the email address at last is working.

Greg Hughes: Right, so if you have questions or thoughts or concerns or ideas, then give us a shout out info@runasradio.com. We'll be glad to hear from you and we may even read some emails on the air, as they say. We'd really like to hear from you.

Richard Campbell: Yeah, let us know if we're doing the right things here, if we're hitting the issues that are important to you. Speaking of that, let's get to our guest. Dana Epp is Scorpion Software Corporation's founder and CEO, researches software security and sets the vision in the convergence of information security principles and practices with digital information asset protection for business. As a security software architect, Mr. Epp has spent the last 15 years focusing on computer programming with a particular emphasis on security engineering to offer a safer computing environment for business. Mr. Epp has been an instructor in the computer information systems department at the University College of the Fraser Valley, and British Columbia Institute of Technology, teaching students about computer programming and information security. He has brought to market various computer security products, including secure operating systems, firewalls, VPN's and authentication devices. His latest research has been on hardening Microsoft based operating systems and protecting information through host based intrusion prevention systems. Mr. Epp has twice been awarded, 99 and 2000, The Community Spirit Award for Business in Recognition of his ongoing initiatives in promoting high technology industries in his community, and won the 2001 Chamber of Commerce Young Entrepreneur of the Year Award.

Mr. Epp is the author of '*Computer Security Concepts: Managing Business Threats in a Wired World.*' A book written to explain at the executive level, how to handle the threats of online risk as companies move to the new digital economy. Dana?

Dana Epp: Wow, that's a big bio. I didn't write that one. Let's shorten it down, because I know you're going to make lots of fun of that.

Richard Campbell: I've suddenly realized that I've got in the middle of the thing, a) the whole Mr. Epp thing, you'd never write that.

Dana Epp: No, I am me. I'm a Computer Engineering geek that has a focus on security. I enjoy and have a passion for doing that for small business, and my goal is obviously to build the best and safest software to allow businesses to get their workflow working.

Richard Campbell: But you really did write a book...

Dana Epp: I did, I did.

Richard Campbell: You've done work at UCFV and BCIT. Of course, we're both in BC, so we're virtually neighbors. You're a little ways away from



Dana Epp talks CardSpace on the Client-Side April 22, 2007

me, but not by much. Microsoft guys wrote that bio, that's the truth.

Dana Epp: I'm not sure if it was Microsoft, or who it was, but I know that there was – one of the things, they've got to make me sound professional, right?

Richard Campbell: Hey, I got it from the 'Security Hardening for Small Business Server 2003 – event information.'

Dana Epp: Ah, yeah;, that would be a Microsoft thing.

Richard Campbell: There you go. So, I think Microsoft guys wrote that. There are I think IT shows.

Dana Epp: Well, that just means that I got to get some better ones that are just more in-tune with the real world.

Richard Campbell: Well, you are so busy, I was just glad we were able to get an opportunity to talk to you.

(00:05:03)

Dana Epp: Hey, no problem and I apologize that we didn't get started earlier, since business gets in the way and making sure customers are protected is number one, but this is always fun too. So, I'm hoping we can get started and have an interesting conversation.

Richard Campbell: We started chatting about CardSpace and OpenID, and a bunch of other technologies at the MVP summit, and I just knew I really wanted to put this on to the show. So, let's start at the beginning, and I know Greg, you're a CardSpace guy too, so...

Greg Hughes: That's true, we are.

Richard Campbell: I may just get out of the way of two CardSpace guys in the same space; we're going to be in trouble.

Greg Hughes: You may have to hold me back on this one a little bit. It's really interesting, CardSpace – and like you work in the security field, my area is really financial services. I work for a company that does an awful lot of online banking software, so CardSpace is something that we got involved with the company that I work at early on. In fact before it was even called CardSpace in some of the early adopter. We've already integrated and done lot of demonstrations with Microsoft on that. I think there's a lot of people out there that would benefit from understanding where CardSpace came from

and what it's all about and what it means to the community.

Dana Epp: OK. Well, that's actually is a really good way to start when we're talking about CardSpace. One of the interesting things about – before we can talk about the technology and everything about CardSpace, let's talk about what the pain is. What the real problem is, that even has Microsoft looking at this, because Microsoft doesn't chase down anything, unless there's a real value to their bottom-line, and at the same time solving customer pain points. What we're talking about is, Passwords. Passwords in themselves are a very weak form of user authentication, and the reason that they're so weak is that anyone and everyone can gain access to those credentials by simply doing something as simple as social engineering through shoulder surfing or asking for – it's kind of funny, there was actually some...

Richard Campbell: What's the name of your dog?

Dana Epp: What's the name of your dog, yeah. What's really funny is this, a guy went and took some Belgian chocolate, and they walked around of New York, and they said, "Hey, I'll give you this bar of chocolate, if you'll give me one of your passwords." And the funny thing was, over 60% of people they talked to got chocolate. So, think about that for a second, right. These people are willing to give – and here's where it gets worse, as we have more and more of a digital convergence from everything. So, we have our bank login, we have our user logins for our work, and we have our stuff at home, and we have our emails. We end up having more and more and more passwords, and Gartner Research says that, on average there's over 20 passwords that people have to remember. No one's going to remember 20 different passwords, especially as it starts getting more complex, and you have password requirement policies that are saying things like, "You need to have over 12 letters, and have set numbers and punctuation, and you can't use the same one for the last 20."

All that gets too hard, so what are people doing? They're using the same password everywhere. So, it becomes an even bigger problem, because now when I've given you that bar of chocolate, if I can just go and try probably 10 or 15 sites online, chances are I might well get into one of those, and I can now act on your behalf. That's where we start getting into a problem, because passwords have no way of identifying who is really at the keyboard at the point of time they want to enter in their credentials to do something. So, how Greg is talking about banking, well that becomes an even bigger problem, because well if



I can log in as you, and I can facilitate some sort of banking transaction, that could be really, really bad. Now, on the flipside of that though, what we get into the problem is just that, when we look at all the security paradigms, some people have what we call throwaway passwords, it's sites they really don't care about. They go to Pizza Hut, and they say, "Come logon to our site," and you get some free points, they probably don't care about those passwords as much. So, we end up having those, that they're just so used to using the same passwords, they put them on a site that's probably not as secured as a bank might be, and we start getting into these problems. Sometimes you call that Risk Based Authentication, it's like we only want to authenticate and really the important sites. If we could just do that, life would be a lot better, because why do we need a password to be on Flickr? Or, why do we need a password to be on some other site, and we start seeing systems like Passport as an example, where we can now have one piece of identity, that allows us to login to a 100, or 200 or 300 different sites, but the problem is, it's still tied to the same password credential. Someone can capture those credentials; I can now act as your behalf on all these different sites.

So, now enters CardSpace. What the problem was is that Bill Gates went to an RSA conference years ago, and said, "Passwords are dead, let's deal with it and what are we going to do." It's actually kind of funny, because if we take a look at some of the quotes that Bill Gates has ever done, and there's all the funny ones about, '640K will be enough,' but the ones that always got me was, 'Passwords are not only weak, they are huge problem in that, the more you get at them, the worse it gets.' He says that at RSA, and people started thinking going, "Hmm, yeah he is right. Bill Gates talking at RSA, we take that as we want to." But, on the flipside, what ends up happening is, yeah they're thinking about something, and what was the result of that, what was called InfoCards, is now called CardSpace and what that is, is that looking at the problem of this whole aspect of password credentials of the keyboard loggers, so there's again going to be shoulder surfing, or what have you – or worse yet, there's just the yellow sticky notes put underneath the keyboard, because no one puts them on the monitor anymore, because they were told that's bad, so they just hide them under the keyboard now. The reality is just, what CardSpace gives you the ability to do is, that it's a new identity management system that allows you to control your privacy while accessing sites.

(00:10:23)

Now, is there something for Windows login in that, no not yet. But, what it's designed to give

you the ability of doing, is having – there's two different kind of scenarios I like to talk about, that is where you want to control your identity and your personal information when you connect up to some resource you may or may not trust, and then you'll have something where there is a vendor or client or business or somebody that needs to be able to trust you, and there's something that's called self-issued cards, and manage cards. In the manage card, you might use the scenario as, let's say you go to your favorite website, let's say it's a book selling site or maybe it's a shopping site, and you're a frequent user there. They might have an association with you and they know who you are, and they have the ability to issue you a card that belongs to you. If we take a look at it, think about when you pull out your wallet from your back pocket, or a woman pulls it out of her purse. How do they guarantee who's who in the zoo, they pull out their credentials, the credentials are going to be the driver's license, they're going to be their loyalty card at the bay, it's going to be their MasterCard, and they might have some other types of cards, maybe their BCIT student card, and different locations might trust different credentials.

So, if I go in and – Dick Hardt has a really, really good presentation on Identity 2.0 which is the scenario of where are we going and what's it going to accomplish, and he is the example of, let's say I'm going in to go buy a bottle of liquor in a liquor store, it's up to the liquor store guy to decide which credential he's going to trust, when he asks me to prove my ID. So, I might pull out my BC ID and that might be enough, but will my BC ID be enough when I'm buying something in let's say, Germany? They don't know what their credential is, it's up to them to make a decision if they wish to accept it or not. What's nice about that is that, I can decide what I'm going to present to them at that point in time. So, when I go to a site like Flickr as an example, if they have CardSpace support, I can say I'm going to allow you to see this card, this is my personal identity card that I've created in itself, because it's got some certain information that I want you to have such as my email address and my username, but you don't need any other stuff like my address and so forth etcetera. You can have what are called, optional credentials that you would provide to them.

So, at the end of the day, what CardSpace does is it provides that facility to have a wallet, and you can have a wallet of different kind of credentials to allow you to login. Then there's some Whizbank technology in the backend that will allow you to communicate in a secure manner, and provide that information that you need. So, they can say, "Hey, you're at the bank and as this



is VanCity Credit Union, you need to use your VanCity identity card or your information card to login here," and how'd you get that, well it was issued to you from some secure mechanism.

Greg Hughes: Now, that's different than you mentioned Passport a little while ago, very different. Passport, I don't have any control over what information is being sent by the Passport centralized service to some vendor or company.

Dana Epp: Right, and the other part is that, Passport is something that's stored in the cloud. So, it's out in the internet and it's managed by Microsoft at all times, and as you go and login to whatever site, if it's Passport enabled, it will go to Microsoft servers and determine, "Hey, I need these credentials, is this the right password, if it is then give me all the information that belongs to Passport." Whereas, with CardSpace, instead of it being handled in the cloud, it's actually handled at the location that you're at, and so when you go in and someone challenges you for credential, your wallet pops up and you decide which credential are you willing to present to that site. The option is a part of that, is that the technology in the backend says, "Hey, these are mandatory credentials," such as maybe your email address and your name, and maybe it's your age, maybe you have to give a little proof what your age is, although that could easily be forged, but at the end of the day what happens is, is that depending on the type of card that's being used, you can say, "Here are some optional claims." We need to make life easier when registering into the system, like what's your favorite color and whatever other information might be in there, your address and so forth.

What happens is, is that you are then in control of what information goes to that site, and better yet it actually tells you, here is what's mandatory, here is what's optional, you decide what you want to provide to them.

Richard Campbell: At least, you have that choice at that moment to say, "No, I don't want to provide that information, I know what you're asking, and I'm not willing to give it to you."

Dana Epp: Exactly, and in many cases, there might be ability where, depending on what's there, you can issue different cards. So, like I have for my CardSpace – my wallet, I have an online identity, which is what I've considered an anonymous identity, where it's a site I don't trust for anything, and that's got certain information that I can track from an auditing perspective, like I use as a special email address and so forth. Then I also have one for a more trusted site, I have a couple of manage ones that were issued to me, and what that gives me the ability of

deciding is, well which one am I going to provide, which ones can I provide? Because, some identity providers aren't going to accept certain types of credentials, but at least I can decide what's there, and if they don't accept what I'm willing to provide to them, then we decide not to do that handshake and we walk away from each other, and no one is the wiser, there's no personal information that's passed on.

(00:15:27)

You go to Passport as an example; actually I just used Passport last night. I was booking some airfare on Expedia, and there was Passport support there to take my credit card. It scared the hell out of me when I logged on, because I haven't been on Expedia for a couple of years, because I usually use the travel agent, and it had all my information, right there and there. It was all pre-populated, stuff that I didn't even want Expedia to have, but it was too late, because I signed in to Passport, and it passed it on to Expedia. You know Passport had a lot of failings, but the idea was sound, and that was the idea of, "Hey, we want to be able to have a single identity to be able to use in multiple places. I don't want to have 50 passwords; I just want to use one." But, where the failing is in my view, and it is just my view. I know a lot of Microsoft people would disagree with me, but I think the biggest failing of Passport is, besides the fact that Microsoft controls it, and it's extremely expensive to get into the Passport clan, is the whole aspect of, it's all controlled by a single password credential. So, if I have a Keylogger on site, and I capture that credential, I have now got access to everything and it's scary, because if you think about my – all the access that I have as an MVP, my MSDN subscriptions and my MVP access and all my Beta connect site stuff. If someone was able to get that credential, oh my god, the access that they would have, and what I would be liable for, under all my NDA's. I would be in a lot of trouble, which is why I'm yelling at them, that they need to get CardSpace and issue an MVP card, but that's another story.

Greg Hughes: Now, in the financial services industry, as we mentioned, there is a risk of having a financial transaction executed on an account by a malicious person or by a fraudster, as we call them. But, even beyond that, that's sort of a one time occurrence. If somebody was to transfer or somehow take \$500 or a \$1000 out of my bank account for example, it's something that would be quite painful, but eventually I would recover from it. The other real risk is identity theft, that's the kind of thing that's very difficult to recover from. So, we're talking about identity and access management in financial services. We quite often talk about the financial risk, but the



bigger and probably longer term risk is really about personal identity.

Dana Epp: Well yeah, the whole aspect of authentication across the gambit is kind of interesting, because you have the end user who has their privacy concerns that needs to be dealt with. In this scenario, we're talking about here the financial institution has their risks and you have everything in between. Something I've never understood in this space is, we can solve this with technology, but security is not a technology problem, and it's a business one, and it really comes down to understanding the risks to the users, and the risks to the businesses. As an example, when you're doing transactions like you're talking about. Logging in to go and see how much money you have in your account, that's a privacy issue, I don't want everyone to see, but to the bank, they probably don't care too much. When the bank is care is that, the point where I transfer funds to another account, because are they liable or not, who's at fault for that transaction occurring, and that's where you realize – talking about that risk based authentication piece. It's like, you might have something that says, "Look, we use a standard password for the user to login to see their information, but anytime that they want to make any changes, or they want to take out money or they want to do something, we require another level of authentication.

So, it might be that we'll allow password to login to look at your account, but if you want to do any kind of transactions, you're going to need an info card to provide that transaction to occur.

Greg Hughes: Then hearing you say that, this warms the cockles of my heart, because that's actually exactly the space that I operate in, and I have a team of developers that build software that does just that. So, I definitely agree and recognize the value and then the risk. The thing about risk assessment and risk management is that, it's called risk abatement. One of the reasons people use online banking and Expedia and a variety of other – Amazon and other infrastructure if you will, is because it's quick, it's easy, it's convenient and it's there. A risk managed approach I suppose allows them to continue to be able to take advantage of the benefits of doing things online while still offering a reasonable level of protection.

Dana Epp: Yeah well, security is about risk mitigation, not risk avoidance. So, at the end of the day, when we take a look at everything that's going on, we have to try to understand what is acceptable to us. What's interesting is this transaction has what's acceptable to both parties, so what's acceptable to me as a user, like what

am I willing to let the world see or let the world access. Whereas the bank might say something to the effect or the website that's doing the transaction will say, "What do I care about to protect my business, because at the end of the day all we really want to be able to do is, exchange our transaction in whatever way we are, exchange to gain access to that information and know that it's the right party who's doing that."

(00:20:10)

When we get online, we don't have that same thing, it becomes extremely easy to act as the identity on someone else's behalf without them knowing. So, if I can be a Russian hacker, that's being able to get your credit card information, which I can use on Amazon to make a purchase which I will then transfer over to a buddy of mine, that's in Canada. Well, what ends up happening at the end of the day is that, we have crossed jurisdiction issues in the world of the internet, where laws are so slow to try to keep up, and at the end of the day, everyone just gets hurt by it, and no one can win out of it. But, what we're starting to see, and I think what's getting better is, we're starting to see people say, "Okay, we get it. We know there is this problem, how are we going to manage it?"

So, CardSpace is one of those steps forward, and it's nice because it's embedded directly into Vista, so anyone who's going forward has it built into their systems, you have the ability of actually downloading a secondary piece in XP as an example. There's CardSpace selectors, that are now being written for browsers on different platforms, so we see support now in Linux, and in OS X for the Mac, and what's nice about that is it's just the start. Who really cares what the technology is going to be, maybe Microsoft is going to win, maybe they won't, but the idea that people are now realizing that we have privacy concerns for the end user, and that the identity should be controlled by them, and not by silos at the store, be it an online store or what have you.

That's starting a mentality shift, and so as we start moving forward, and we can start using our digital identities to actually do more and more transactions. We're going to have more and more fraud and crime that's going to go, because of course criminals go where the money is. So, what a risk quotient will be and what we're willing to accept now is going to considerably change over the coming years, and technology is going to have to catch up. So, we're starting to see some of that like OpenID, I know we talked about that at the beginning of the show. Here is a scenario where people are saying, when you're doing postings on blogs, and you want to have



access to certain types of sites, we might have the ability of being able to provide a single URL as an example, as your identity. It's not a perfect solution, because it's easy to spoof URL's and control the network data flow, and now people have come in like Kim Cameron, who have stepped up and said, "You know what, we can solve this." This is where CardSpace in conjunction with OpenID can support the mechanisms to provide the secure transaction to guarantee that you are who you say you are, and that URL is a trusted URL, that you can take advantage of, and now we can use that technology that's in there. What's nice about that whole scenario is Microsoft didn't invent that technology, they've just been able to apply one piece, where they seem that they've been able to add value in the wallet for the CardSpace and deploy that out, so then we used another technology, that we'll use in this case to be at the protocol layer to -- is it to communicate to these different types of sites, and allow for a login.

Greg Hughes: I think one of the really complicated things about matching up that people, process and technology – those three portions of the pie if you will is that, in order to meet those business needs, the technology quite often needs to retain a level of usability that doesn't ruin the experience, and I think Microsoft has done a pretty good job with CardSpace, even in this initial release in terms of doing that. Maybe, you could discuss a little bit, what is the experience like for an end user?

Dana Epp: Well, I'll talk about the experience as I see it, and I see it probably little different than let's say someone who's doing transactions from home, it's your mom or your dad, that's trying to deal with it. The way I see it, is anytime I go to a site that is CardSpace enabled, it gives me the opportunity and it prompts me with my wallet, which is basically just a secured desktop which has a listing of the different types of credentials that I have in my wallet, what I call the information cards. Some will be managed, some will be self issued, and I get to make a decision of which cards I wish to use to send to that identity provider, and the identity provider in this scenario ends up being that website I'm at. I can then decide to select which one is there, and then it can tell me, "Okay, here are the credentials it's asking for."

Actually, I'm using the wrong terminologies, I'm sorry. It's not what credentials that they're asking for; it's what claims are they asking for. It's saying, "Hey, I want your email address, I want your first name, your last name. I want to know your age; I want to know your address." There's lots of different pieces of the claims that they can be asking for, and I can then decide which card I

want to select, and when I select that one, it then gives me the option to review it to make sure which information I'm sending. So, it allows me to control it from the privacy perspective, what I'm willing to share with this site, and then it allows me to login, and then it passes that on. What's nice about that scenario is, I haven't had to enter in any password credentials to do that. Now, to be fair, I always have a pin assigned to all my cards, just because, if for some dumb reason, I didn't logoff my machine and I walked away, I don't want someone to sit on there and act as me by basically having my wallet and using that credential to show it to other people, which could be bad.

(00:25:06)

Richard Campbell: Yeah, I'm just thinking that laptop theft is still going to be an issue here.

Dana Epp: Right, and that's where security is going to come into play, where you're going to use other pieces right? So, in the Vista world, we have ability of using BitLocker, so we have an opportunity to lock down the hard drive, so that people aren't going to be able to pull the drive out and get access to your card, because obviously, if your cards are stored on disk, they're stored in a secured manner, but even still if I can get access to the hard drive, am I going to have an opportunity to get access to it. With technology like BitLocker, that's in Vista, I don't have those risks, because if they try to pull it out, it's not going to work, they need to have the TPM or in my case, I use an external USB that stores the information, and what ends up happening is that they're not going to be able to get that. Securities, you got to have a layered defense approach. So, we want to secure – well it's on disk, so if my laptop goes away, I'm not going to fret about it as much, and then I have my pins that are on my cards to guarantee that if someone's there with an open session, that they're not going to gain it, and then of course, they need to have the card as well to be able to provide the login facility.

Greg Hughes: You've mentioned self-issued cards and managed cards. I don't know if we've gone into real detail about what the real differences are between that. The self issued card would be one that I create for myself?

Dana Epp: Yeah, in CardSpace, you have the ability in your wallet to create different cards, and the cards could have different persona. So, in my case, like I was saying, I have basically an anonymous card, which just got a bunch of – what I would consider fluff, It's not that it's fake data, but I use my online handle, and I use an email address that I consider a throwaway one that, if I see I'm getting spam from that, I know



that, hey possibly my information was accessed from that site. I might not want to trust that site anymore. So, what ends up happening is, is that I can create those cards for myself and when I go to these sites, I can use those cards to login. Now, the site has the decision if they want to trust it or not. It's just a step above on the password side of things, because how do you really trust and you know who is who in the zoo. On the flipside of it, you can have a managed card where using other types of business process, the business can make a determination on, how are you who you say you are, and how can I guarantee that once I've made an association that I can trust? I can issue you a card and I'll store all the claims and all the information at the server. So, basically the card just has – we have one for our own office, we have a card that we've issued that's specific to access certain information. We're just kind of testing the CardSpace world and how that all works, and what's nice about that is that the server issues that card, and I have it on my machine, I cannot login from anyone else's machine unless I export my card, and import it into their wallet to get access to that information, and what's nice is that the server, and I can revoke those access at the server side, and then that card is kind of useless to them.

The analogy I like to use all the time when I'm talking to people about this is, imagine you have a loyalty card, using storage – so like we're in BC here, so we have, Save-on-Foods has there loyalty card, where you get points every time you use it. It would be nice if they could allow you to have an identity card – an information card that allows you to login to Save-on-Foods and it's tied to your actual physical card that you're always using too, so you could buy things online, and you know that it's your card, because they've issued you that card and there's that association. Now, you don't have to worry about having your passwords, you don't have to worry about someone else logging in and using your points and etcetera, etcetera, etcetera. It's probably not a site I'm going to visit that much, maybe once a year, so chances of me remembering my passwords are going to be pretty hard. But, if I have my card, I just pull it out of my wallet when it's prompted, select that card and I go on, and it works.

Greg Hughes: Now, one of the interesting things with managed cards that I noticed when we were working with it early on, is if it's a managed card that's issued by ABC bank for example, and I go and I visit other sites then, the ABC bank card doesn't light up if you will. It's grayed out.

Dana Epp: That's right. What happens is that the managed card is provided for their identity

provider. So, unless the other providers have technology in place to allow us for the exchange of those type of credentials, you won't be able to see it, and what's kind of nice with CardSpace is that, when you login or you get prompted and your wallet comes up, the cards that it is willing to accept, or that they believe is willing to accept are highlighted for you, and the ones that it expects that are going to be the ones will be best suited for the site, they actually get provided first. So, from a user experience point of view, it's just a couple of clicks, and normally you'll be able to select the first card that's highlighted there, because that makes sense to you. Depending on how you go now, we might get to a world where we end up having 20-30 cards and it might get a little more difficult, but none of us are there yet to really know if that user experience is going to change. But, you're right, you go to a card – like that Scorpion card that I have, no one else can use that card at any other site. They can't even issue those claims, because the Scorpion sort of doesn't even talk to that identity provider, so they have no mechanisms to validate it or approve the identities to that.

(00:30:02)

That could change, as an example imagine if the government of Canada decided to issue information cards, and that card might be able to be used at any government branch at any place. Well, those are various different websites that might exist, and they might have the ability of talking and working with other vendors such as the passport office or maybe with banks, where they're going to say, "Hey, if you can provide me your government information card, we'll use that as a claim we can trust." So, as systems be able to start being able to trust each other from an identity provider point of view, we'll actually have the ability of having – what I would consider stronger claims, that come from sources we trust, that we can use across the board.

Richard Campbell: In some ways, you've just abstracted the whole Passport model. Right now we're hubbed around Microsoft's information. The fact that we can have these third party cards, that other people can then trust, means you can choose what pairing you want to make. That whole idea of affinity between these different groups is quite a powerful concept.

Dana Epp: It is, and I think what we'll see is if we find better ways of managing this whole aspect of handling it, I think we're going to be able to start having our physical ability to have what I would consider a traveling wallet. Right now, in version one of CardSpace, it's tied to the machine that you're at, and there is a way of exporting the cards and then importing them in, but it's not a



Dana Epp talks CardSpace on the Client-Side April 22, 2007

clean way. What I would love to see as we come to a day and age, where maybe we will be able to cleanly store it on a smart card or on a USB key, in a way that it's trusted. So that, I can have a roaming identity, like in my own business we built Two-Factor Authentication systems, and the reason we do that is that, things like CardSpace just aren't quite yet ready for doing things like Windows login, or being able to have mobility, so that I could go and use Richard's computer to login to access my mail. That technology is just not quite there yet with CardSpace, but I bet you, that the team at Microsoft, they've already got that all in their roadmap, and that version two and three, as we start to see them come in, will allow us to have that flexibility. So that, we could have that momentum and that ability to be mobile, and still have this kind of strength in their cards, so basically being allowed to carry our wallet everywhere we go.

Richard Campbell: It sort of ties in to a thought that Greg and I were talking about before the show, which was the whole when your laptop gets stolen, now what? How do you clean up from those cards, get them disabled. How do you even know what they are?

Dana Epp: What happens when your wallet is stolen? What happens right now? You have to call up MasterCard and Visa, and say, "Hey, I will need you to revoke those cards, and I need you to send me new cards." You get the same scenario. Sometimes, with the selfish cards, it gets a little more different, but I also see there's other technologies that can be used there, that Microsoft just hasn't tapped in to. So, if we take a look at the digital locker room as an example, it has ability to store your EFS and BitLocker keys, your encryption keys basically in Vista. You can actually go store them up in the cloud now in a secure manner, in something called the digital locker. What would be nice is, is if you could do the same thing with CardSpace. Hey, I want a secure mechanism to store my wallet somewhere else, so that if I need to get access to those cards, I can and I can then make a decision if I need to revoke them or not.

Richard Campbell: And I'm not going to do it often enough, that I'm going to make it easy for me to get to it. So, give me some difficult security obstacles to make that happen, because when I do need it, I really need it and I need it to be secure when I don't need it.

Dana Epp: Yeah, that's one of those things. I guess it gives – we go right back to where we started this whole conversation about how password security in itself is a very weak form of user authentication. That gets compounded when we start looking at everywhere we're going to.

So, if we only go to a site we go to once a year, what's the chance we're going to remember that password? In this day and age, it's actually pretty easy, and it'll tell you why. The reason it's pretty easy is because they all use the same damn password on all 50 sites they go to, but that's not the right way of dealing with our protection of these things. So, they have two ways of going about it, you have a really good 'Forgot Password' link that you can manage to send back to those email addresses or better yet is that we're able to use a card that we can always issue – get challenged with later, and we'll have it when we need it.

Richard Campbell: Dana, we've gone around full circle nicely on I think the whole client's side of CardSpace, and we've run out of time. I think we need another show to talk about the server side of CardSpace. How am I supposed to implement these things?

Dana Epp: I think it would be fun to do. Now, a lot of stuff that I would be talking about, we will obviously have to – depending on when we do the show, we'll look at that, because some of the stuff especially on Longhorn Server, there's some really neat sexy stuff, and I'm not sure what we can talk about, when we can't yet. But, I'll make sure we get that all cleared up before we do that next show.

Richard Campbell: Thanks very much Dana, we'll talk to you next time on RunAs Radio.