



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 #015
(Transcription services provided by [PWOP Productions](#))



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

[Music]

Carl Franklin: From runasradio.com, you're listening to RunAs Radio, the weekly Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Carl Franklin, introducing show #15, with guest Dana Epp, recorded Thursday, July 12, 2007. RunAs Radio is produced each week by PWOP Productions, offering professional media and podcasting services online at pwop.com.

Richard Campbell: Hi, this is Richard Campbell and you're listening to RunAs Radio and I'm here with my co-host, Greg Hughes.

Greg Hughes: Hello Richard, show #15.

Richard Campbell: 15, yes sir. We're coming up on the four-month mark if you can believe it.

Greg Hughes: Yeah, it's been a fun ride. I'm really enjoying myself.

Richard Campbell: Well, we're just getting back into the groove of recording regular shows again after having a month's worth of TechEd shows.

Greg Hughes: Right.

Richard Campbell: I guess we could talk about this now, but we're going to TechEd Europe.

Greg Hughes: That's right in Barcelona, Spain.

Richard Campbell: That's right.

Greg Hughes: Never been there before.

Richard Campbell: Well, I was at TechEd Europe last year in Barcelona, but that was for the Dev Week. Now, we're going to go for the IT Week.

Greg Hughes: Yeah, the IT Pro Europe Week. I'm really looking forward to it. I've never done just an IT pro-type TechEd thing, so I think that will be pretty interesting.

Richard Campbell: I'd say an interesting dynamic splitting the weeks up like that. Rumor has it that they're going to do it in the US soon too, so we're going to get some practice there, but you and I are

going to be really busy because we're going to host Speaker Idol there.

Greg Hughes: Yeah and that's going to be a whole lot of fun. Speaker Idol at TechEd US was really pretty cool, just the opportunity for people who were not presenters at TechEd, but to get up on the presentation stage in front of an audience and then get voted on a lot like some show that everybody in the world is probably fairly familiar with and...

Richard Campbell: We definitely borrowed the idea.

Greg Hughes: Tell me if I'm wrong, but as I recall, after the several hits if you will of Speaker Idol, the one person who came out the end as a winner actually got a TechEd speaking slot for next year.

Richard Campbell: That's right. That's exactly the idea is they are looking for a speaker for TechEd, so the overall winner of the Speaker Idol is going to get a speaking slot at the next year's TechEd.

Greg Hughes: What a great opportunity actually to be able to see somebody speaking, people speaking that maybe you wouldn't see otherwise in order to be able to evaluate them and realize, "Hey, wow, that's somebody that really should be speaking at a show like TechEd."

Richard Campbell: I totally agree and another interesting angle on this is there is only five minutes to do your presentation.

Greg Hughes: Yeah, that's tough.

Richard Campbell: And then really dense content. I am blown away by how much these guys get into five minutes.

Greg Hughes: It was really pretty amazing and it was a lot of fun to watch. The fact of the matter is if you flub things up, five minutes seems like a long, long time and if things are going well, it's like it's over all of a sudden.

Richard Campbell: Flashes by.

Greg Hughes: The people that really seem to make it work or the people that you could tell that they had their five minutes of content rehearsed, they've



trimmed it down, they cut the fat, they added here and there, and they took feedback very well because one of the key things judges are providing feedback because in the finals they really were looking to make sure that that feedback was followed.

Richard Campbell: Absolutely. We keep the same judges through the whole contest and those guys are trying to influence and improve those speakers. That's a very interesting feedback. Those guys have a fascinating view on the whole process.

Greg Hughes: Yeah.

Richard Campbell: So, besides Speaker Idol, we're also going to do a bunch of panels and in fact I guess this is a good opportunity to call out to the listeners. If you'd like to see a panel discussion, or rather hear a panel discussion, we're going to have time at Barcelona to do at least four different panels, so if there's particular topics that you'd like us to pull some experts together on and talk through these issues, here's your chance. Send us an email, info@runasradio.com, and we'll take your suggestions, see if we can pull those panels together and the show is the second week of November. We're going to be recording those four shows over the course of a week in front of an audience and we'll see what happens.

Greg Hughes: And I'm sure we'll have an opportunity to speak with other people, individuals at TechEd Europe just the way that we did at TechEd US. It will be a lot of fun, really looking forward to it.

Richard Campbell: All right, I got an email for you, and this one is a little confusing to me. You can probably help me understand this. It's from a guy named Allen Thompson and it was sent to the info@runasradio.com email address, what he's referring to -- well, let me read this. "Hello there. I was interested to see your article on Lockergnome as the use of IP tracking for me is a worrying development." Now, where does Lockergnome fit in the equation?

Greg Hughes: Ah, that's your confusion. Gotcha. So, of course, my blog at greghughes.net -- if we post a new show, well, I'll write some of my thoughts and comments and refer to the show and my blog entries in some cases, some of the technology entries are actually syndicated and are published on

lockergnome.com, which I believe you've met Chris Pirillo before.

Richard Campbell: Yes, of course.

Greg Hughes: Chris is a great guy. I was talking with him yesterday and he's just a funny guy and quite a personality.

Richard Campbell: Wicked smart, actually.

Greg Hughes: Very, very smart. By the way, he has a terrific live video show going on now. I don't know if you had a chance to check it out.

Richard Campbell: I haven't seen it yet, no.

Greg Hughes: It's really pretty darn cool. He's doing an awful lot of interactive video stuff that's really worth checking out, but lockergnome.com, spelled the way it sounds, they actually have an information technologist-focused blog. They have a Windows user-focused newsletter and syndicated so you can get it on your RSS reader if you're the subscriber type, a variety of different methods for getting that information, all of which is published on at least a weekly basis, some of it on a daily basis, terrific information. So, anyway, that's the...

Richard Campbell: That's the whole Lockergnome angle.

Greg Hughes: Yeah.

Richard Campbell: Because I don't understand why he's talking about an article on Lockergnome rather than about the show directly, but it was obviously a topic that we addressed, the geolocation.

Greg Hughes: Right.

Richard Campbell: Let me give you the rest of the email here. "There seems to be an increasing number of websites that redirect you to pages specifically designed for the location where you are and believe me, that can be a bad thing. For instance, try accessing Abercrombie and Fitch website from the UK. The prices are in pounds, but they are much more expensive than the US where the numeric amount is the same, but they're in dollars." That to me sounds like a bug.



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

Greg Hughes: Yeah. That's interesting. I can honestly tell you Richard that I have never gone to Abercrombie.com and I probably never will.

Richard Campbell: Oh. I can't believe that, Greg. You're so hip.

Greg Hughes: As I'm sitting here in my geek T-shirt with my blue jeans on, right?

Richard Campbell: I'm in Canada so I often deal with the fact that I can visit websites that may or may not recognize that I'm in Canada. The first thing I do at any unusual ecommerce site is check will they ship to Canada. Answer is usually no.

Greg Hughes: Right.

Richard Campbell: But, you know, that's reality. I think there's nothing wrong with geolocation per se. It's trying to help you out, but it is up to the developers to build decent software they can deal with the reality of like Allen refers to. What if you're an international traveler? You happen to be in France right now, but you want to make a purchase that will be delivered to your home in America. You've got to be able to do that, so smart websites are going to be able to handle that, but I wouldn't give up on geolocation just because of that.

Greg Hughes: Yeah. I can't call that -- and he's referring to the interview that we did with Bill Varga from Quova.

Richard Campbell: Right.

Greg Hughes: Which I thought was a great interview and it's a lot of really cool information. This isn't a geolocation problem, this is a how do you use a geolocation information. You could use geolocation, you could use browser user agent strings, or things that are not related to geolocation. You can basically profile your customers and then not drive your workflow efficiently and not think through all the different use cases. In the case of this particular online retailer, I think the concern is probably valid especially when you look at the exchange rates these days.

Richard Campbell: Oh absolutely.

Greg Hughes: But I would say that I think geolocation is a great tool and IP Intelligence is a terrific tool, but whenever you use any tool, you need to use it the right way. If you've got a flathead screwdriver and you stick it into a Philips head slot, it may work, but you may rip up that screw head.

Richard Campbell: For sure and we can't forget part of the discussion around the geolocation was regulatory compliance. There are going to be cases where products should not be shown to people from outside of certain locations.

Greg Hughes: Absolutely and business doing business the way they do it isn't always a function of technology quite often. It's just a function of business.

Richard Campbell: Yeah.

Greg Hughes: Funny how that works.

Richard Campbell: Yeah. The number of times, I read shipping facts that leave out the fact that Canada is a foreign country. It makes me understand we still got a ways to go.

Greg Hughes: I think Allen's point about making sure that -- he does have a valid point, by the way. I'm not trying to minimize that at all. I think that choice is a pretty critical thing for consumers to have.

Richard Campbell: Yeah. They expect it -- and you as a business owner -- don't mess that up.

Greg Hughes: Yup. If you drive it down somebody's throat, you force them to fit into a certain slot and they don't feel like they fit there, you can pretty much count on the fact that they're going to walk away.

Richard Campbell: Right. All right. We better get to our interview.

Greg Hughes: Yeah. Let's do that.

Richard Campbell: All right, Greg. Let's introduce Dana Epp. Of course, he's been on the show before, way back in show #3. Dana Epp is Scorpion Software's founder and CEO, researches software security and sets the corporate vision -- good Lord, Dana. What a bio. Look at this thing.



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

Dana Epp: Let's make them go back to show #3 if they really want my bio.

Richard Campbell: Yeah, because it goes on and on and on.

Dana Epp: To keep the identity and access control stuff.

Richard Campbell: But you are a security guy through and through. You've done it for years now.

Dana Epp: That's right.

Richard Campbell: We promised we'd get back to CardSpace because we've ripped through that first half-hour just talking about the client side parts of CardSpace and since that show back in April, we've done -- we've talked to Richard Turner as well, which I'm sure is a guy you're familiar with.

Dana Epp: Yes.

Richard Campbell: And he drilled in at some different angles on it, a little more history bits and so forth, but I've not yet really heard the real solid story of for me as an IT guy how CardSpace is going to work on my servers in my network. How am I going to implement this? Is it only for my website?

Greg Hughes: Not to mention why am I going to implement this?

Dana Epp: Those are all very, very good questions, and the answer is yes. All right. I'll get more serious.

Greg Hughes: Okay, thanks. That was 30 minutes.

Dana Epp: There you go.

Richard Campbell: Yeah, let's go. We're out of here.

Dana Epp: When we talk about CardSpace on the client side, it was easy to try and explain and try to get that association that what we're doing is we're trying to work with this Identity Metasystem that allows you to treat your identity as something you as a client controls through what we're talking about the CardSpace wallet and so in that last

session, we talked about how that all works on the user's experience, but today let's talk about how that works for the business, the organization that's driving this. When we were talking about some of the scenarios in the last show, we were kind of talking more about the personal user experience and what I want to talk about the business is how does it work through all the different systems and servers and the whole aspect of identity and access management. So, when we talk about CardSpace in the server, what we're really talking about is something called an STS, which is an acronym for Security Token Service, which is really the meat, the bread and butter that controls the tokens behind the scenes on how system work. The whole point of what an STS can do for you is it allows you, especially on the side when we're talking about the managed card, is it gives you this power to let you drive the authentication mechanisms across systems, which could give us the power of having the really nice Single Sign-On that we've been looking on or sometimes they call it SSO. Is it for websites? Yes, definitely. That's actually where CardSpace seems to thrive really well right now.

Greg Hughes: Sure.

Dana Epp: Because there's a lot of personalized STS's that have been built there. We see it with Community Server. We're seeing it with -- actually, Kim Cameron was posting months ago about a PHP STS that already existed out there.

Richard Campbell: Cool.

Greg Hughes: And of course he has CardSpace enabled on his blog.

Dana Epp: Yes, he does.

Greg Hughes: As do a number of others.

Dana Epp: Yeah. We got into the world let's say after Directory and you will integrate that directly into the system.

Richard Campbell: Not so much that I want to -- what I really want is not have to create another identity. That's what you keep telling me. I'm going to go to Single Sign-On. I've got all of this identity information in Active Directory right now. How do I get it to CardSpace?



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

Dana Epp: More importantly, it's not just about how to get it to CardSpace, how can we provide that information that it could be used across to many relying parties.

Richard Campbell: Right.

Dana Epp: So, you know how we're talking about one of the nice things with CardSpace is that we no longer have an identity silo. So, we don't have our login credentials in 15 different spots. We can have them at one. Well, the idea is Microsoft's been building some technology like ADFS, which gives us the thing called federated services that has the ability to allow you to have this kind of mechanism.

Richard Campbell: Acronym definition please, ADFS?

Dana Epp: ADFS, the definition. Well, you know, the easiest way would probably to go and search on Google and give it the big nice scenario, but the way I would explain it's an architecture that gives you the ability to have federated services, Active Directory Federated Services.

Richard Campbell: Right, so this is ADFS, Active Directory Federation Services.

Dana Epp: Federation Services, sorry, and it allows that whole point of federation and the technology called WS-Federation, which is the Pset is really important here, which gives us the ability to exchange credential information across certain types of boundaries. What's interesting is that ADFS already exists. It exists in Windows Server 2003 R2, but the problem is that the current implementation is using something called WS-Federation Passive Profiling, which is not compatible with CardSpace yet.

Richard Campbell: Oh.

Dana Epp: Which kind of sucks.

Richard Campbell: Yeah.

Dana Epp: But on the good side of it, we have a new version of Server coming out, Windows Server 2008. There's talk that they'll have Active Profiling, which is what CardSpace uses, which hopefully will let us have the ability then to use CardSpace with our AD infrastructure.

Greg Hughes: You say there's talk of that.

Dana Epp: Well, I wish I could say it is definitely in stone.

Greg Hughes: Right.

Dana Epp: I honestly don't know the answer.

Greg Hughes: Sure.

Dana Epp: I wish I had the answer. I'm not a Microsoft employee and we all know that next February is when their launch date is, but the actual final bits, are they in there, are they not, I don't have the answer to that right now.

Greg Hughes: Well, it's a fairly complicated system that's not quite done yet and so obviously things change over time.

Richard Campbell: Maybe we need to define more clearly the difference between a passive and an active system.

Dana Epp: You know, I don't have the expertise to be able to explain that on how that side of it works on the nitty-gritty.

Richard Campbell: Right.

Dana Epp: I just don't know. The way that I look at that and how I understand it though is that CardSpace is the active system to back channel communications and it's actively being processed, but I'm not sure if that's the right way and how they define it, so...

Richard Campbell: Okay, and this is all these WS specifications that we've been working on for quite a while now.

Dana Epp: Yeah. Well, that's one of the things. Microsoft is trying to drive some of the technology that relate to the server type thing, but they're trying to use standards-based systems here. They're not just inventing something just for themselves.



Richard Campbell: Right. Isn't CardSpace a completely open specification, anybody can implement it?

Dana Epp: Yeah, v1.0 is already out there, the full documentation and it's been implemented like there's a wallet selector in Firefox, there's support in OS X already and Linux. So, yeah, you can use these kinds of cards from the client side on different operating systems and there's nothing to prevent from the STS side of it, the Security Token Service. Nothing prevents that from running on the server side as well, which means that in the identity ecosystem, nothing prevents CardSpace to be run in an exclusively Mac shop as an example.

Richard Campbell: Right.

Dana Epp: And Microsoft actually has its own implementation, I quite frankly like it because it's default-deployed in Vista, right? It makes it for the masses of people out there to be able to be used, but think about it from the business side of things. To be able to have an identity ecosystem that allows you to transcend the boundaries of operating systems to do Single Sign-On without complex mechanisms that have been out there that the enterprises have been using, so now small businesses and enterprises can have the same type of Single Sign-On across websites, across domains, across identity selectors, and that all could be very, very useful and as it grows and the new specs get out there because the first one's already published and now it's there and anyone can access it at Microsoft's -- I think it's available on MSDN actually -- you can get that information, but their version 2 is already in the specs right now and lots of different groups ranging from Sun and Novell and Apple and Microsoft and Liberty Alliance, they're all talking, they're all trying to find ways to make it all work and it's interesting because Microsoft's not the only player in there. There are lots of different systems out there that are trying to find this mechanism where you can have one source for identity control cross there we were talking for the show things like OpenID as an example is something that provides some mechanisms.

Greg Hughes: Right.

Dana Epp: And then of course you can grasp on CardSpace support for the back channel actual authentication piece where you can actually

use your card to be the piece that does the authentication to the OpenID provider, which then allows you to use OpenID to log on to 15, 20, 30 different sites you might have access to.

Greg Hughes: You know, I think the concept is really this loosely coupled -- the term used in the industry now is this metasystem concept of loosely coupled cross platform, platform-agnostic if you will, capability for a Single Sign-On or a single provider capability. Isn't it really a lot like it used to be with -- if we look at it from a hardware perspective, isn't it kind of the way it used to be with video cards way back in the day? You used to have to program, your application on an old school computer had to know how to speak to each specific video card and then eventually came the idea of abstraction, building drivers and layers in between, so you that have some commonality in a single API that the operating system can deal with and then that allowed video card manufacturers to write drivers. Right?

Dana Epp: Yeah, for sure. What's interesting when we look at the authentication mechanisms, like earlier I was talking about this idea about the silos, no one wants to be able to say, as an example, "Hey, I'm working at XYZ Company and I've already got a credential that I use for logging in there," and now I happen to work with when I need to deal with my healthcare stuff relating to that, so maybe I have my healthcare provider, which is part of the insurance that I have with my company wants some access to some of my information. How do they get access to that? Do I have to have two different login accounts, one for checking my healthcare records or getting information there, dealing with billing, etc., etc., etc.?

Greg Hughes: Right.

Dana Epp: But why can't I use the same one that I'm using? What if the healthcare provider who works with the company has a mechanism to allow you to work together when it comes to the authentication piece? So, now, you just use your same business credentials to get that access or the company store that might be available to you or partners that you're going to be working with. So, instead of having 15, 20 different passwords, you have one that can transcend the boundaries. Maybe they don't have Active Directory in their organization, maybe they're a Linux shop and they want to use



something else. Well, that's fine as long as they follow the specs and what's nice about this is at the end of the day, it's just XML services in the backend.

Dana Epp: Sure.

Dana Epp: There's lots of technology, WS-Trust, there's WS-Federation, WS-Security stuffs here, but those are all open standards, which you can take advantage of and use across any of them.

Richard Campbell: I think the important part here is this is really old plumbing.

Dana Epp: Yeah.

Richard Campbell: It's going to be transparent to us as operators of it that this is how it negotiates, but you don't need to know that protocol any more than you need to know HTTP anymore.

Dana Epp: That's right.

Richard Campbell: All right. I got my server. I want to use CardSpace. You know, we had it easy when we talk on the client side about those managed cards, but now I actually need to make one. What am I talking about doing?

Dana Epp: To make an actual STS?

Richard Campbell: Yeah. Well, to make that managed card that I want my customers to use.

Dana Epp: Okay. Well, so the Security Token Service, it becomes their responsibility to issue the card and they're going to store the keys that are in there. If I can take a tangent for a second, I'll give you an example of how you can actually see this working now without affecting your business and that is -- a lot of people don't know this exists, but Microsoft over at live.com has some research that they're doing on STS's. You go to -- what's the URL now? sts.labs.live.com I think it is, yeah, and what that is, is it's the Live services STS. It's a Security Token Service and you can go register your servers with them and they become the STS that provides providing and you can control with CardSpace by logging into those systems. So, they're showing us an example. I think they have warnings the last time I looked, it was a couple of months ago, but it was like a huge warning saying, "Warning: This is exploratory

research. Don't be running this in your corporation for full-time authentication," but you can see what they're looking at doing is having this ability to have this generic STS that can communicate with different systems at all times, so you can use your single set of cards and they can be deployed and managed and worked with through a single chokepoint if you want it to or you could mesh it out and have failovers and all that kind of good stuff.

Richard Campbell: Do you see this is the way this going to happen going forward is you're going to use it for a service provider for your STS or you're going to run one yourself?

Dana Epp: Well, I think it will be dependent on the type of business you have and what kind of risks you have. I don't see enterprises wanting at any time right now to delegate their authentication pieces out to third parties.

Richard Campbell: Right.

Dana Epp: But I do see places like salesforce.com as an example or these other software as service businesses where they realize that, "Look, we've got these web entities, but we've got to talk to other web entities and how can we all work together?" They'll be able to trust an STS, the relying party, so the identity provider, the IDP is going to be what you want it to be. Could it be live.com? It could very well be. It could be your own ADFS system at your corporation. It could be your own home STS box. It really comes down to how you want to control it.

Richard Campbell: This reminds me of certificate server then.

Dana Epp: Well, yes and no. We all know what the complexity of PKI has always been at and one of the difficulties with the whole aspect of PKI outside of certificate authority trust, which has its own set of headaches for people to deal with, you know, all the sites that are self-find versus using proper CAs and now with the browsers saying, like IE 7 now just goes up and says, "Warning! Warning! This is not a good site. Don't go there."

Richard Campbell: Yeah. Here's the red bar of fear for you.



Dana Epp: Yeah, exactly. Of course, now, in Vista, it's even harder because you can't go up and trust the CA. Because it runs in protected mode, it won't let you install the root CA into your browser. You actually have to run it as an administrator with protection mode off before you can actually add those certs so it becomes even more cumbersome for a lot of businesses and organizations. What's nice about the plumbing as we've been referring it to for this whole aspect of the STS is that it's all done over standard protocols like HTTPS or HTTP and it communicates in a way that it's understood by both ends to allow you then to create the levels of trust and that's what we're talking about here. Authentication is nothing more than someone has to trust somebody else and how you want to delegate that authentication and who to will really come down to the different types of providers out there. So, as an example, in our last show, we talked about what if the government issued a card? Well, the government would have to run an STS and it would have to be a well-thought out and protected STS because the last thing you'll ever want would be a managed card server to be compromised because then that's like compromising every single passport user in the world.

Richard Campbell: Right. Right.

Dana Epp: Not passport as Microsoft, I'm talking the government, right? If it's your medical card or it's your passport or whatever that is, Social Security numbers, SIM card, whatever. A breach in that kind of system could be devastating, whereas it's not as devastating if someone breaks into a passport office and steals a couple hundred passports.

Richard Campbell: Yeah, as opposed to getting them all, which is really what you're talking about there.

Dana Epp: Right, and so the STS is sort of something like ADFS where supporting an STS like that would have full control because Microsoft's obviously going to reduce the attack surface in a way that will make that a functional system and scalable to the kind of masses that are needed out there.

Richard Campbell: Now, as a company, am I always going to want to issue a managed card or will I be happy with non-managed cards?

Dana Epp: I think it depends on the type of resources you want to protect. I think at the end of the day though from a company standpoint, you want to be able to in many cases delegate authority and authentication maybe to roles or groups that might belong if we're talking on the enterprise side of things. You might as an example have -- you know how we're talking about healthcare, maybe you'll have a special card that is your personal or business identity card, your staff card, but then you might have a different card for access to more sensitive resources such as if you're an executive and maybe you have access to things like PerformancePoint or CRM systems or what have you. You might need to have a different card to authenticate to those types of systems because maybe we don't want to have that -- now, what prevents you from having a single card? Nothing does. They might just have a defense-in-depth posture where they'll layer on different types of authentication mechanisms and they might even be from different service, right? So, we might have the HR system that manage the employee system might be different than the IT system that manage access to sensitive resources, but they'll all be able to talk together using the same protocol.

Richard Campbell: Right. Okay, so getting back to the fundamental question of what we have to do to run this ourselves. Right now, we really can't.

Dana Epp: Well, you can. There are a couple of things you can do. There are things like Community Server right now and actually if you've got devs in-house, there are things like the simple STS, which is a .NET-based source code pool that allows you to write your own STS to work on your own system.

Richard Campbell: Right. I guess what I'm really saying here is that Microsoft hasn't shipped an STS for us to run in any form yet.

Dana Epp: No, not as today's date to my knowledge.

Richard Campbell: But Community Server, that's Telligent, right? Rob Howard's company.

Dana Epp: Yeah.

Richard Campbell: Has actually written a version, an STS version for Community Server.



Dana Epp Digs Into the Server Side of CardSpace July 18, 2007

Dana Epp: That's right and there exists a load like there's a PHP implementation, I know of a Perl implementation. There's a couple of C# ones up on DotNetJunkies, sorry.

Richard Campbell: Right.

Dana Epp: There are lots of base code out there that exists on simple STS's, which would then let you do things like run and issue your own managed card like as an example even Scorpion Software, we have our own STS, which we built and we're contemplating rolling into our authen build to factor a communication system so customers could actually deploy not only authen tokens, but authen cards if they wanted to, not in our current release and not in our next coming builds, but it's something that we're seriously contemplating because we see this as a need and because we already have agents that support things like ISAPI filters and the Web Servers and we got support for RADIUS and things like that. We could actually use CardSpace in some of those spaces to be able to provide a different token technology as an example, in this case, card technology to provide authentication.

Richard Campbell: Yeah. You know, we've got a lot of choice here, but still the conservative IT guy in me says this is still too new.

Dana Epp: Yeah.

Richard Campbell: That we're still innovating a lot, we're still trying to figure some things out. I might try this on an experimental site, but I'm not going to roll it into primary sites. I'm not going to count on it overall.

Dana Epp: Yeah.

Richard Campbell: And it's not that it's a bad thing, it's just early.

Dana Epp: It's early. What we're seeing right now is that version 1.0 is not the end of where we're going with this. The thing that I always like to joke about is you know it's not mature enough authentication system for your corporation if you can't control your Windows login.

Richard Campbell: Right. That is the basic measure, isn't it?

Dana Epp: Yeah, it is because if you can't provide a mechanism to log in to your desktop, what gives you authentication mechanisms? And I say that across boundaries. There are a lot of good uses for a lot of those technology out there, things like CardSpace and OpenID and Yadis and all these different systems that are out there. They're great if maybe you just want to control web access and what's nice is I think CardSpace is a mature technology now that can be used for things such as web applications, so if you have a company that might be let's say exposing reseller or partner data to somebody and you need a mechanism to control the authentication, CardSpace would be a good answer to that now.

Richard Campbell: It's a better solution than, say, FormSpace authentication.

Dana Epp: Oh definitely, way better than having a standard username-password mechanism and CardSpace supports the user-password selector type system and the user could do that without a need of a managed card.

Richard Campbell: Right.

Dana Epp: They can use their own card. You register with us with your card and that would then give you access to our system. That could work now and that works now and we see lots of examples of how CardSpace works in that realm because that's just where it fits right now.

Greg Hughes: In that case, a username and a password plus a card, correct? Even if it self-issued.

Dana Epp: Yeah. Well, what happens is that the user when they create their card in the selector, the equivalent is instead of having the password, you have this key, the set of keys, and this key information gets stored at the server and what happens is that they now have a way of initially knowing who's going to do what and that that card belongs to you and that you're authenticating as who you say you were, but now you don't have to type a password in.

Greg Hughes: Right, but I do have to actually have my device...



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

Dana Epp: Have your card.

Greg Hughes: Some kind of physical possession of that device that holds that electronic card.

Richard Campbell: Correct.

Greg Hughes: Right. So, there's something I have kind of factor if you will, is there?

Dana Epp: Right, and you can even tie that down a little more because you could lock it down with a PIN so that you know that it's actually you that's using that card at the time of authentication.

Greg Hughes: So, being vendor agnostic, platform agnostic, and just looking at the real world today, if we had to, say, between now and the end of the weekend put together a real world actual, full-blown, and we'll say it's on a website application where we could put this into play and make it really work including an STS where we wanted to manage the identity and actually do the issuance and manage all of that, what's the technology that we could grab off the shelf and put together and plug together to actually make it work right now.

Dana Epp: Well, on the client side to redeploy, you could use the CardSpace that's built directly in a Vista or download the CardSpace support that's for IE on XP. That would give you some different card selectors out there for Firefox and what have you. For the client side piece, that would be done. On the server side, you need to have some sort of STS and so you could grab any one of the open source STS's out there like we were mentioning there's a PHP one, there's a couple of C# ones, Perl ones. You would install that on whatever web server or system that you have that you want to provide that on to and they'll have mechanisms to then plug that into the FormSpace off their authentication mechanisms to manage the cards to do the login facilities there. I know that you guys, you have in your other radio show where you talk about on the .NET side of things or the dev side. You've done a lot of interviews already on how developers can add that according to their own sites, so which means that you could literally deploy this in less than, you know, 100 lines of code from the server side, you know, how complex you want to deploy this and anytime you're

going to build like an STS, you really need to sit back and think about it.

Greg Hughes: Sure.

Dana Epp: I'd use what's out there now because the whole aspect of securely storing the information on the system would be too critical to me, so if you're going to go write it yourself, you'd need to really understand what the risks are and of course how to deploy that. As an IT pro, well, most people don't want to write their own STS, they'll use what's there.

Richard Campbell: Yeah.

Dana Epp: And deploy it as they see fit, right?

Richard Campbell: I can also see that in the next year and maybe less than that. In the next year, we will have standard STS's that we'll use from Microsoft...

Dana Epp: Oh yeah.

Richard Campbell: And any other platform they're working from.

Dana Epp: Even Windows Server 2008, when it comes out in February, if it doesn't have the full support for the WS-Federation in active mode, I'll guarantee that these guys are going to be working their butts off to get you like the first rollup Service Pack or even just a patch level.

Richard Campbell: Yeah.

Dana Epp: Because the guys over there like Kim Cameron and his team are working really hard on making sure that they got support on there and I think they would be fiscally irresponsible if they didn't have a business solution for such a great identity system.

Richard Campbell: Well, it sounds like the uncertainty we're hearing is really about everybody raising to deadline. Now, that hard date is out there, everyone gets jumpy now.

Dana Epp: Yeah, and you know, it's like I was originally kind of reluctant about the idea of



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

actually coming and speaking on the server side because like I've seen a lot of this stuff already working in action and it's like, "Well, is it going to be in the final release or not?" I don't know the answer to that and I don't think it would be right to pull the MVP card out and say, "Okay, well, let me know because I need to tell the community." I just don't think that's right because they have enough pressure on their bunch right now.

Richard Campbell: Yeah.

Dana Epp: They don't need me trying to weasel out a definite yes or no in there, although it depends who you ask. Some say it'll be in there, some don't so I don't know the answer to that yet.

Richard Campbell: But I think the message we can pass to the listeners here that's a pretty solid one is there's no way I'm going to be deploying this as my primary login to my internal network.

Dana Epp: No, not yet.

Richard Campbell: We're not there yet. It's going to come so I might as well keep my head up.

Dana Epp: Yeah.

Richard Campbell: But if I was involved in a team whiteboarding a new extranet site, like you said, a supplier site or something like that, I would be thinking CardSpace on it.

Dana Epp: Yeah.

Richard Campbell: And you know, if forms authentication is an option like, boy oh boy, guys, let's not commit to that now knowing it's going to be there for two or three years. Let's go to this new relatively rough, relatively young technology now knowing that will be ready for what we're going to get in the new incarnations of ADFS and the new servers in the next year or two.

Dana Epp: Well, and think of the architectural implementation issues that you get into like if you back and use a standard username-password, which we know is a weak form of authentication in the first place, and we move just up to CardSpace in its own silo as it is right now, like you build your own STS to work as is, the interesting

piece of that is when it's time that you might move that to ADFS or you move that to some other kind of STS that's out there, the plumbing is still going to be the same so the user experience won't change.

Richard Campbell: Right.

Dana Epp: You might change how or what machine or which system they're going to authenticate to...

Greg Hughes: Right.

Dana Epp: But as far as they know, they go to a site, they have to provide their card and get logged in.

Richard Campbell: I think that's the really powerful message here is that if I can get guys using cards today, they're not going to have to change from that for years.

Dana Epp: Right.

Greg Hughes: And again, the beauty of standards, right?

Dana Epp: That's right, and here's the funny thing for some of these businesses is as they're deploying this out there, they might decide, let's say today as an example, they're running this on IIS and they're having this all driven on IIS 6.0 and, hey, next thing you know, they're going to move to IIS 7.0. Well, you know, backend, do they really care? They know that their standard websites are going to work, that ASP.NET is going to work and so too will the authentication mechanisms. They know the user experience won't change no matter what the backend is going to be. If you do the username-password, yes, that is true, that still is the same, but you lose any of the forward momentum abilities that you'll have.

Richard Campbell: And the ability to carry that database of username and passwords forward is going to be very, very tough. You shouldn't do that now.

Dana Epp: Right, and down the road, as you start growing that depending what kind of the services they're providing in this kind of extranet environment, you also can gain all the extra reporting and auditing abilities that will come with ADFS or



whatever STS's out there that they decide to mature up to as the server side technology matures.

Greg Hughes: Yeah. The classic way of new technology coming out of the past where standards were not being established and not being put in place, it's a little bit different now. The programmers have always been concerned about contracts breaking and from a programmatic standpoint, you know, Microsoft releases a new version of something and all of a sudden my software won't operate anymore.

Dana Epp: Yeah.

Richard Campbell: Oh, that never happens.

Greg Hughes: No, not anymore, but with WS-Star and with a lot of the standards that are in place including in this CardSpace world, that concern is at least I think is pretty seriously mitigated and it's a similar thing for the IT pros who are out there and are saying, you know, "You release something new and all of a sudden, these two systems won't talk to each other anymore." It's a different point of view, but ultimately it's the same type of problem.

Dana Epp: Yeah. If you go and use a static username-password system now, but you then down the road want to decide to use something like CardSpace, one of the other luxuries you get on there is that the whole ecosystem allows it to move to other server technologies and other pieces that your standard username-password won't give you.

Greg Hughes: Right.

Dana Epp: Or better yet, the ability to have the IDP utilize other sources because that's all built in now. We know the clients that all works, by just having even the base plumbing in there now you will be able to extend that to whatever system you want down the road and it won't affect the end user or the developer for that whole login experience.

Greg Hughes: Right. So, again, one standard across all the technology, that loosely coupled methodology of chain-linking things together so they "just work."

Dana Epp: Yeah.

Richard Campbell: Well, and the openness so that anybody can step out whatever company could stop making their product, then somebody else can step up.

Dana Epp: Right.

Greg Hughes: From a technologist perspective, we mentioned earlier that -- and I think it's a fairly true statement even if it's unfortunate that there's a hesitancy to adapt to new technology, I mean we just keep it that simple. What information is there that can convince technologists and IT pros today that this is something that maybe is worth taking advantage of and we've talked a little bit about it sort of, you know, what you get out of it, but what are some of the things that can help build confidence that says, "If I do take advantage of this today, is there anything that can cause me to not have to worry quite as much as maybe I've had to worry in the past?"

Dana Epp: Hmm. Interesting question.

Greg Hughes: We've all had our experiences with, you know, we adopt a bleeding edge or a leading edge technology and I would say we're not bleeding on this anymore, we're sort of leading, right? And we've had our successes in that area and we've had our failures in that area. I'm curious as what your perspective is thinking about it from that direction. What is it about what's available now?

Dana Epp: Well, it's a fine line because when you take a look at it from an IT pro's side of things -- as a developer, I love new technology and wanting to see it because it's easier, it's better and of course when we start talking about a lot of this, we have a reduction in lines of code, which means a reduction in possible lines of bugs.

Greg Hughes: Right.

Dana Epp: But on the flipside of it from an IT pro's standpoint, we have to look at it as we want mature technology that works. We don't want to be sitting there and be beta testing, especially something like authentication, which is critical to the business at hand.

Greg Hughes: Absolutely.



Dana Epp: We don't want to be just replacing it haphazardly without understanding what the true benefits are and what the drawbacks are when things go wrong and one of the things that I think when we talk about authentication that balances that whole issue is the rich reward that relates to what we're trying to protect or more importantly, especially when we talk about security, what risks we're trying to mitigate. We said this in the last presentation and I'll say it here is that the standard username-password system is sluggish. It's so weak. It's not even a system we should be actively trying to support. We need to move off of that and everyone knows that. There's enough stats out there to put that in perspective, but now you have to balance that with, "Okay, then what do you replace it with?"

Richard Campbell: Well, and what's surprising here is that, and I guess this is the best endorsement we could ask for is already the client side is cross platform and the only other thing that's cross platform like this is username-password.

Dana Epp: Yeah.

Richard Campbell: That's pretty compelling.

Dana Epp: Yeah, but on the flipside to that is that it's not a compelling solution if the answer is cross platform the way that it allows anybody to act on your behalf with **a)** not without your knowledge and **b)** without you having any way of controlling that.

Greg Hughes: Exactly.

Dana Epp: So, you know, the idea of something like CardSpace as an example gives you the ability to say you know it's you using those credentials because there's a lot of other things that have to go on before someone can act in your behalf with a card. We look at other technologies that are out there that seem to get a lot of following right now like OpenID. A lot of people say, "Oh, it's so great because now we're associating our URL to our identity of who we are. We can control that URL," and then 9/10th of the people out there with this OpenID have it from some place like AOL.

Richard Campbell: Right.

Greg Hughes: Right.

Dana Epp: You know? Or some provider who quite frankly I don't want to put my trust in. You get a lot of the blogs that are supporting OpenID, but they're on servers. What if that server is compromised, right? That's the ever-ending question and we want to use these systems -- well, that's no different if all it is, is if I can compromise that one server and I have accessed every single person's identity in the world, that's not a practical solution from an IT pro's side of thing either, not saying that that would happen, but, you know, it's one of these things we need to consider because when we talk about businesses and we talk about how we have to be responsible to our own stakeholders, one of the things we need to think about it if we're going to deploy something, how does it help us for what we have now. So, that question to me is as easy as saying we know that username-passwords work, but they're weak and that in this system where we are today, it's very easy for someone to pretend they're someone else and because most of us have remote access, that gives confederate access to critical resources. We need a better way of knowing the identity of those coming in. So, that will be why we'd want to move to it. Well, how do we do that and how we deploy that in the way that makes sense? Well, CardSpace now works from web-based entity stuff. So, if you have things like let's say SharePoint servers, web applications and so forth that you can put this type of stuff in front of it, makes total sense to do it. It's not going to help us with our current system for the local login though.

Richard Campbell: Not yet anyway.

Dana Epp: No, not yet anyway. Yes, good point. On the other side of it though, there are some other benefits that we get that I don't think a lot of people consider and that is things like the idea of having Single Sign-On so you'll log in once and you'll be able to get access to anything and everything you like and access to password management as it relates to defunct passwords, passwords that would expire, passwords that have to be changed because of password policies, and what have you. The cost especially in an enterprise, they're significant when you think about how many times people have to manage the whole password problem. What if we can eliminate that for all of our extranet partners?

Greg Hughes: That's a good point.



Dana Epp: Right? These are things from an ROI standpoint. You got to measure and decide if it makes sense to do that and I think if you weigh that all together, that gives us the ability to decide do we stay with what's currently working, but might not be perfect versus do we go with the flow and integrate new technology that solves the problem. Is it a pain that's large enough in our business where we're required to take action?

Greg Hughes: Yeah, and I think the beauty of the username and password, if you can even say there is a beauty to it, is that from a strict usability standpoint in terms of end user acceptance, it works for them in terms of I know that I can go to the website, I can type in my username, type in my password, click the Submit button, and I'm in, right? When you start introducing new layers and other levels of complexity, it gets to be very difficult. With the Microsoft CardSpace support, one of the beauties of it is, is they have done a lot of, you know, graphical user interface work and they have tried to make it as - it's not really even dumbed down. It's just as functionally visual I think is a better way to put it as possible in order to find what's really needed, which is from a usability standpoint, an acceptable replacement for the username and password.

Dana Epp: Yes, and part of that is because the idea of when you have a username and password, it's something you'll typically set and forget and now I think it's a big flaw because I know I have this regular basis and I don't consider myself any better or worse than most people on the Internet, but I forget so many different site passwords because I go there once a year.

Greg Hughes: Right.

Dana Epp: It's not a site I go to. With CardSpace, the nice thing about that is I still have my card with me, so I'll remember. There are lots of facilities I've seen now where they don't even have a really good password override or change policy that allows you to get access and the perfect example I have is that as an MVP on our monthly conference call with some SBSes out there and we have this chat, this online chat system drives me nuts because every month I forget what the password is. Every month I have to contact the admin and say, "Can you please reset my password?" And I'm sure he's getting annoyed and I'm getting annoyed because I

don't simply want to put a weak password on there because it's my MVP credential that's not tied to my password account and I just have so much other things that are more important on my mind that remembering the chat password that I'm going to use for half an hour once a month just isn't the highest on my list.

Richard Campbell: Not going to make it.

Dana Epp: It's not going to make it and I keep bugging them and say, "Look. I'll give you the 10 lines of code on how to deal with emailing me a new temporary password just, will you implement it?" Their reason for it has to do with privacy policies and I understand, but whatever, but when I look at something like CardSpace, you get another benefit from that. It's got the same ease of use as the username-password, but allows you to have the identity to be controlled by you, which means that you then have access to it when you want it, when you need it. One of the other pieces to that is when I use a username and password on Facebook as an example, that username-password hopefully if I'm being mature enough and not reusing stuff isn't going to be the same one that I use at Amazon.

Richard Campbell: Right.

Dana Epp: It isn't going to be the same one, but when we start talking about CardSpace, I could. I could use the same card at all three spots.

Greg Hughes: Right.

Dana Epp: But they're different identities. They're like different associations and so I have that level and I don't have to worry about trying to remember three different sets of credentials.

Richard Campbell: Right. Well, Dana, always a pleasure. I think we've pretty much pounded that down to the ground. It's going to be interesting to talk about CardSpace again in a few months when we see more stuff finished and ready to go.

Dana Epp: Yeah.

Richard Campbell: It's a fun time though, isn't it?

Dana Epp: It is. You know, I love being on the edge of this and some stuff. I can see this being -



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

- the way we're going to go moving forward in the future, it would be interesting to see as it matures on the server side how vendors -- and I'm not even just saying Microsoft here, I'm saying all vendors because I think as we start looking more with things like WS-Federation and we take a look at WS-Trust and we take a look at how this all works together and how we can actually have systems all talking together, it will really be a nice day when we can actually use our mobile credentials. One of the things that we didn't talk about or we talked about last time that we didn't get to deal with was the whole aspect of cards can't be mobile, right?

Greg Hughes: Right.

Dana Epp: We don't have the ability of having our cards carried with us.

Richard Campbell: Right.

Dana Epp: Well, since that show, a vendor has come out now with the ability to have on a Smart Card be able to carry your credentials now.

Greg Hughes: Ah.

Dana Epp: And it's very interesting. They actually have a workable solution now and what's nice about that is that it means that you can get a managed card issued onto a Smart Card and then you put that Smart Card into any machine with CardSpace, CardSpace will recognize it and load it up and you can then use it on that machine and then you got to pop it out, obviously a problem being is you need to have Smart Card support in the machine, but outside of that you now have the ability to have that, so we've already answered one problem that we were talking about in our last show.

Richard Campbell: Yeah.

Dana Epp: Which was this whole aspect of can we move our identity around with us.

Richard Campbell: Yeah, just a couple of months later and we have an answer.

Dana Epp: We do and so now, we talk about on the server side, in three months, four months from now, I think we'll at least know what the story is there and if it's not from Microsoft, it will

probably be some other third party vendor saying, "Hey, guess what?" Actually, you know what? I misquoted. You can look at companies like Ping Identity that's doing it right now. They have the conduit as an STS that works with AD Federation and everything else that's on there as a third party solution.

Greg Hughes: Absolutely. It will definitely be interesting to see what happens between now and the end of the year.

Dana Epp: Yes, sure.

Greg Hughes: The other thing I think that will be really interesting to see is Microsoft and Ping and the OpenID community, what people come up with in terms of something that will in a very clear and concise way visually and in a good explanatory fashion show IT pros and business people the real value of this in a way that they can swallow all in one sitting.

Dana Epp: Yeah.

Greg Hughes: One of the difficult things about this is that it's easy to talk about the philosophy and some of the technology behind it, but it's one of those things where I think it's a little bit more difficult to say, "Here is exactly why and here is exactly how it will work for you." It will be interesting to see what people will come up with over the next few months.

Dana Epp: Yeah, and we have to break the shackles as it relates to people's understanding and acceptance of how these credentials are going to be used. One of the problems is everyone wants to keep the credentials to themselves. They're not willing to want to share. So, we need to be able to have identity providers and relying parties to be able to communicate in a meaningful way and not worry about the trust aspects being out there. We need Google to be able to trust an IDP that might be a Microsoft or out of Microsoft's server and we need Amazon to be able to trust Google, so that we all can have one central system that we can decide which way we're going to communicate and it doesn't matter who owns the credential because at the end of the day, we just want the user to be able to get access to resources, but we want to know it's that user.



Dana Epp Digs Into the Server Side of CardSpace
July 18, 2007

Greg Hughes: Or to validate who the user is, hence, the concept of federation.

Dana Epp: Yeah, that's the whole point of it.

Greg Hughes: Absolutely.

Richard Campbell: All right, gentlemen. I think we better call it.

Dana Epp: All right. Well, thanks again for inviting me to come on again. It was fun.

Greg Hughes: Thanks Dana.

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