



Hansel minutes

Hanselminutes is a weekly audio talk show with noted web developer and technologist Scott Hanselman and hosted by Carl Franklin. Scott discusses utilities and tools, gives practical how-to advice, and discusses ASP.NET or Windows issues and workarounds.

Text transcript of show # 39

October 30, 2006

Identity

Scott and Carl talk about digital identity and related technologies.

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



Our Sponsors



<http://www.codesmithtools.com/>



<http://www.nsoftware.com/>



<http://dotnet.con-sys.com>





(Music)

Lawrence Ryan: From Hanselminutes.com, it's Hanselminutes, a weekly discussion with web developer and technologist, Scott Hanselman, hosted by Carl Franklin. This is Lawrence Ryan announcing show # 39 recorded Monday, October 30th 2006. Support for Hanselminutes is provided by CodeSmith tools, makers of CodeSmith. An extensible template-based code generator for .NET. Hanselminutes listeners get \$100 off CodeSmith professional with Coupon Code HM100. Online at codesmithtools.com and by /nsoftware red carpet subscriptions. The most comprehensive solutions for adding connectivity to your .NET and ASP.NET applications, with components for every major internet protocol. Online at www.nsoftware.com. Support is also provided by .NET Developer's Journal. The world's leading .NET developer magazine online at www.sys-con.com. In this episode, Scott and Carl talk about identity.

Carl Franklin: Hi, this is Carl Franklin you are listening to Hanselminutes. I am here with Scott Hanselman, hi Scott!

Scott Hanselman: How are you sir?

Carl Franklin: Identity, CardSpaces, is the topic today.

Scott Hanselman: Was that your Sean Connery?

Carl Franklin: Identity.

Scott Hanselman: Today Carl and I will just show you all the history, Identity 2.0. Yeah dude, this is all about CardSpaces, because we've been, -- we talked about doing a .NET Framework 3.0 show but we all know that the Framework is too big to do in a short Hanselminutes double speed, 20-minute Podcast so we are going to do it in chunks.

Carl Franklin: We also know that, it's really not a Framework .NET for 3.0

Scott Hanselman: Yeah, it's kind of, it's a collection of pillars.

Carl Franklin: New features.

Scott Hanselman: These were the new features, so we've got CardSpace, we've got Windows Presentation Foundation, and we've got Windows Communication Foundation. So, Avalon, InfoCard and Indigo were the code names. So, at Corillian we are really interested in CardSpace

because you know we do online banking, and banks are always getting phished. They are always getting attacked by people who get their names and their passwords stolen.

Carl Franklin: Right.

Scott Hanselman: And we encourage people to have stronger passwords, we encourage people to have passphrases, right add a space and have a big long password that's like 20-30 characters long. But these are still just things that you know that can be stolen from you, you can be tortured and they could -- you could give them up. And generally identity on the internet is broken. You got identity theft, there is spoofing, and they're in the middle things, and there is evil Malware that could be running on your machine, and it's pretty clear that the user name and password mechanism is overwhelmed. I mean just the fact that we've got Password Manager Programs, programs with a super password that are set up to manage your other passwords. It doesn't really work, right?

Carl Franklin: Yeah.

Scott Hanselman: So, the whole idea is, what's a better way to identify both the user to the site and the site to the user. Because a lot of times you go to a site and you don't know if you trust this site, maybe it's a blog, I don't want to go and sign up on a blog, I don't know about you but I don't want to sign up with a blog and give them yet another user name and password just for the privileges of leaving a comment.

Carl Franklin: Exactly, the less sign-ups I can do the better.

Scott Hanselman: Exactly, so then we get down to these kind of main sign ups and then of course, Passport, Microsoft Passport was kind of an attempt to centralize all of that, but the problem was it was managed by Microsoft. It wasn't the fact there was Microsoft, but it was the fact there was a single entity that will handle it. They were basically saying, just us your user name and password and we will come up with a tricky way to single sign you into all these different places.

Carl Franklin: And we will keep your Credit Card number on file and all your business information, all your personal business info...

Scott Hanselman: Right, we'll hold all your stuff.

Carl Franklin: And the response was a resounding, yeah, right?



Scott Hanselman: Yeah, it worked technically like I used it for Expedia and for eBay and that was pretty much the extent of it but I just didn't feel comfortable with it because, you never know, I don't think that password was fished successfully, but it's easy to make a site that looks like the site that you want to go to. So, phishing is a problem, and of course, we've seen Firefox 2.0 and in IE 7. They have built in anti-phishing stuff. There is a good reason just to install IE 7 right there; I've put IE 7 on all my relatives' machines.

Carl Franklin: I also think Scott, before we get too far away from it, that one of the reasons Passport failed or .NET My Services is what we're really talking about, was just because of timing, there was a lot of disruption going on, security-wise at that time.

Scott Hanselman: Yeah, it was kind of the end of Web 1.0, and the beginning of 2.0, the bubble occurred and it was a fairly disruptive thing and it was not exactly easy, frankly to integrate it if you ever tried to get your Passport to work, STK was a little tricky and just when you get it working another STK came out. So, the real issue, here is what the guys at the CardSpace team and Nigel Watling is one of the guys that's got a presentation I'll point everyone to, is the idea of Identity Silo hell. You get all of these different Silos, where you have an identity at one place but you are not trusted by another, like Amazon is big and wonderful and they use my identity for a number of things. I can make reviews and comments, I can buy stuff but I can't use my Amazon identity or my reputation and use it somewhere else.

Carl Franklin: So, let's talk about CardSpace.

Scott Hanselman: Okay so, CardSpace is basically an implementation by Microsoft of an open and specifically non-proprietary way to represent identity. It's open and non-proprietary in that it uses the WS Stardotstar Technologies, it's on with web services, using XML assertions, using Ws-MeX, that's called WS Metadata Exchange, I like to call it WS TeX-MeX but people don't like that joke -- and using WS-Trust.

Carl Franklin: Scott, I know that anybody can say this is an open standard and then still exploit it for their own personal benefit at the expense of others. So, the real test is, is anyone else besides Microsoft using it?

Scott Hanselman: That's a very good point. So, of course, this is an example of something where Microsoft's done the first and perhaps thus far the best implementation of it, but people are already

getting excited about this. So, for example the guy Kim Cameron at Microsoft, who really promotes this who runs, identityblog.com...

Carl Franklin: Brilliant guy.

Scott Hanselman: Up at Shrinkster/jkm, he runs a blog based on PHP. So, in a kind of an unusual move by Microsoft guys, he ate his own dog food and built a PHP implementation of InfoCard. So, if you have CardSpaces on your machine, the Windows implementation of CardSpaces, then you can go up to his blog and you can sign in and it's using all PHP, no Microsoft stack. So, the idea is that, you would go up to his blog and in this instance, you would be using IE 7 and then you'd have the .Net Framework 3.0 on your system. Remember, that IE 7 is going to get pushed out as a high priority update to everyone and that .Net Framework 3.0 is going to be an optional but recommended update. So, I think more and more, we are going to see this. It's also built into Vista. So, otherwise it's unfortunate that 3.0 is not going to be a high priority update. We are going to see this pushed out to a lot of peoples machines. You go up to his blog and then you visit a regular HTML page. If you did a View Source on this page of the HTML, you would see an object tag, right an object tag is the kind of thing you would use to show like a Flash object. In his case the object is an information card that's saying, I have some requirements that you are going to need to give me. So just like you -- for putting a name and password together on an HTML site, you would say input text equals password, input text equals -- text. And it would put in their name and their password. In his case within the form there is an object tag.

Carl Franklin: I love the Elastigirl thing, what's that all about?

Scott Hanselman: On his site he uses Elastigirl from 'The Incredibles' to represent his very flexible implementation of CardSpace. So, if you basically click on this object the browser will pop up and launch whatever that helper is. So, in the instance of IE 7, it will launch what's called an Identity Selector. it's going to launch the Windows CardSpace Identity Selector and on Windows or on Vista, you are going to get this kind of Curtain of Death, this kind of grey transparent curtain will drop and a CardSpace Identity Application will launch up and let you select a card and in this context, the card is a kind of a Client Side Certificate.

Carl Franklin: Yeah, that's a good thing to clarify that it, isn't necessarily a physical card although it can be stored on a card.



Scott Hanselman: It's a very good point. The CardSpace cards are basically kind of a Client Side Security Token that are going to allow you fulfill some claims that the site will make.

Carl Franklin: It's like a metaphor for a Credit Card or something...

Scott Hanselman: Exactly, it's like handing someone a card because like if I go to in -- you are in Connecticut, right?

Carl Franklin: Yes.

Scott Hanselman: Okay, so , I am in Oregon, so I go to Connecticut and I get pulled over and I show the cop my Oregon driver's license, why does he trust me? He trusts me because Connecticut trusts Oregon. So he says well, I don't know you, Mr. Cop, and Mr. Cop you don't me but I know Oregon and I know Connecticut, so we trust each other because, we trust this third party. So InfoCard uses that card metaphor that idea of, here is something that I have, it is attached and issued by someone that we both trust, a lot like SSL works, right? I visit your site, you use a VeriSign SSL card and then we have this trust relationship. So, you've got this object tag on your HTML page and it's just coded like a regular object tag like a Flash tag or any tag that uses object and it has a certain type that says something, something /InfoCard, the browser associates, whatever the Identify Selector on your system, in this case the Windows CardSpace UI, that pops up this Curtain of Death and the reason, I point out the Curtain of Death is because, this is a new separate desktop, because you don't want to let any Card Loggers or evil things that are kind of snuck into your system, anything running in the tray or some Malware. So, this is the similar technology that they are using in the User Access Control stuff in Vista. They are basically running this in its own universe, its own parallel world on your machine, its own desktop context. So, no other applications get to get loaded in there and it's running in a very limited trust, it does exactly what it does and no more. So we are trying to prevent phishers being able to get into that space and futz around. That -- you select your identity or you create a card, there is two kinds of cards, you can have a self-issued card, you basically create your own cert and there is a little Security Token Service on your machine that basically issues the card to yourself. So this would be the equivalent of writing on a piece of paper 'I am me' and then using that as your identification.

Carl Franklin: Right, if somebody wants to trust you they can but they don't have to.

Scott Hanselman: Exactly, a site would have the choice to say, I am only going to deal with one that has done with a managed card and the other kind of card is a managed card. Now, I am hoping that not only will Windows Live or Windows Live is the re-branded Windows Passport, they will of course implement this and people, who have passports will automatically get CardSpace cards. But I think, like Visa, American Express, these big kind of places that manage your identity, they will issue managed cards. So, if you trust Visa and I trust Visa, then we will have this relationship.

Carl Franklin: And it's interesting because then your Credit Card becomes more usable as a source of identity.

Scott Hanselman: Exactly well one of things...

Carl Franklin: Like a license is now, visually the Credit Card can electronically.

Scott Hanselman: Right and if -- let's say I am going to buy something from Franklins.net. Right now, I go online a make a login and I register and it's all name and password, then I would give you my credit card and I have got two choices, either, I can let Franklins.net store it, without any understanding, about how you are going to choose to store my Credit Card or I just give it to you each time and I have to just fire it across the Internet and I have to keep updating you on things like the expiration date and if I did a managed card rather than me sending you the Credit Card number, I could send you the Managed Tokens, this Managed Security Token and then you could talk to Visa and they wouldn't have to give you the Credit Card, they could just say, oh, this person has decided to pay you \$10, here is the confirmation number and Credits Cards could be removed entirely from the process. So, the number doesn't exist. It's a...

Carl Franklin: And all the transactions happen behind the scenes at Visa.

Scott Hanselman: Exactly and it's all done in a cryptographically significant way. So this Identity Selector back to what you were saying as I call who else has done this. So, they are already starting to see Identity Selectors for other browsers. There is a Firefox one written in Java at [Shrinkster/jkn](#), right now it works on Firefox 1.5 but I am sure he will update it and there is one for Safari at [Shrinkster/jku](#), I think, that as more and more people realize that this is not a Microsoft thing this is an open WS *. standard that they are going to start creating these. I think, we will see all the major browsers supporting an Identity Selector in various ways. I found that CardSpace



1 the one that's built in with Windows to be very flexible. Right now, you do have to store your cards on your local machines and you can move them from place to place. So, I've basically exported my cards and then imported them back at home. In the future, a version of CardSpace is going to support using your USB key, as a kind of a token and then saving the tokens on that key. So, then you would have no store on your local machine, but you will be able to login on any machine and then say, oh, here is my identity. So, you'd basically be using your USB key like you just said as a smart card. So, it would be a poor man's smart card and certainly that would be much more ubiquitous than a smart card itself.

Carl Franklin: This is another thing that came up in my conversation with Kim Cameron on .Net Rocks! which is, RFID tags and as soon as I said, RFID he, -- I could hear the hair on the back of his neck bristle, he said, RFID is not a security device. It's not secure. Anybody with an RFID reader can walk up to you with your FOB and read what is coming out of it and then, give it an answer and so there is no cryptography and there is nothing. You've seen people going around with Laptops with RFID readers and RFID units or whatever they call it, Reader-broadcaster or Reader-writer; I don't know and they can go up to like a Prius, which uses -- I am giving away that people can hack my car now but uses an RFID tag on the FOB and they can just sit there and within an hour they can not only get into it, but they can start the engine.

Scott Hanselman: Right. RFID is just broadcasting a GUID for a lack of better way to phrase it. I mean it's in a no space and no way, if it claims to be any kind of security.

Carl Franklin: Right.

Scott Hanselman: So, yeah, definitely, but the idea that someone could use a flexible token and create something unique to a USB key and turn that into a Smart Card like device, that's a powerful thing.

Carl Franklin: Yeah,

Scott Hanselman: Now, there has been also a number of examples -- there are chunks of code online, will it be in Java or in PHP on how to do these things? There's an example decoder at [shrinkster/jko](#), where you can basically see what was sent; it will actually show you what happened on the wire, because this all happens only under SSL right now

Carl Franklin: Right

Scott Hanselman: And that decoder will show you the assertions in the underlying web services and, <if you like that kind of stuff, you can see it> and there is a very good article at MSDN, at [shrinkster/jkp](#), that will explain kind of step by step how this works, and actually the Wikipedia article -- I know that, Wikipedia is a little dodgy but at the time that I read it it was quite up to date at [shrinster/jkr](#). So many people are getting excited about this. Now, I had planned to enable DasBlog for information cards.

Carl Franklin: Cool.

Scott Hanselman: But, Kevin, Kevin Hammond beat me to it by like, a week

Carl Franklin: No kidding.

Scott Hanselman: He has taken a casadehambone -- that's his website -- it's the casadehambone and that's at [shrinkster/jks](#) and he has taken an instance of DasBlog and he has enabled it for info cards. So, this could really change the way people do identity over blogs. So, leaving comments and he also now uses that information card to log in to the administration of his blog.

Carl Franklin: Wow!

Scott Hanselman: So, in this case no password being required. So, Kevin has enabled DasBlog using this personal private identifier that is sent as one of the claims. Basically, when you're sending an information card, you can insert a series of claims in that object tag that say, "Here are the requirements" you might say, "I'm going to need from you an info card that has first name, last name, personal private identifier and your e-mail address." And each of these claims is described using a URI, a Uniform Resource Identifier.

Carl Franklin: Yup.

Scott Hanselman: You just list these things out in your object tag, saying, "These are the things I'm going to need" And that Personal Private Identifier is actually unique to the card and the site. They are actually using some of the information within the SSL certificate to hook you up with the site. So, if I visited Franklins.net under SSL or Hanselminutes.com under SSL, I would get a cryptographically significant and different Personal Private Identifier. So, that unique ID couldn't be stolen by a phisher, because it's different on a per-site basis. Starts to get interesting now, right?

Carl Franklin: Yeah.



Scott Hanselman: So, for example, we have an application here at work that is a name and password kind of a thing, but we also have this notion of a single sign on, the idea that you might have some other external system that's going to manage your identity. So, we can put in unique identifiers that we call them 'aliases' and a lot of single sign on systems do this. They are basically saying you can login with your name and password or one of these Alias Identifiers and a lot of systems that have implemented this alternate identity, can just take that personal private identifier and use that straight up as an alternate way to login. So, that -- a kind of thing that I think you'll see are sites that include the support for logging in the classic way or in the info card way? So, I could envision time when I might go to Amazon one day, log in with my name and my password and then go to my main account management page, say, associate an information card with my account. Send them an info card and then they would take that private identifier, that personal private ID that's unique to Amazon, because it's a combination of some of the stuff in the SSL certificate and some of the stuff on my certificate and it's going to stick that number, I think, it's like a 32-character long kind of GUID like thing. Stick it in their database and then I could actually shut off name and password support. I would say, "I don't want anyone allowed to log into Amazon anymore by name and password. Info cards only." Then it starts getting interesting. Right?

Carl Franklin: Yeah.

Scott Hanselman: Now, that's just with a self-managed card. One of the things that self-managed cards don't really support is the notion of revocation. This is the idea that you want to cancel your card when someone steals it.

Carl Franklin: Alright.

Scott Hanselman: Now, if Amazon issued cards from their own security token service and they said, "Well, you have an Amazon identity, so, we're going to give you an Amazon card," -- just like, they would give you an Amazon Credit Card with the Amazon logo branded on it. I could go to Franklins.net and say, "Hey! Here's my Amazon card" and if you have a trust relationship with Amazon, you could use these WS Trust web services to actually ask Amazon, "Do you know this guy?" When I hand you an information card and you would say, "And I need these claims. I need this guy's first name, are you going to provide that to me?" and Amazon would say, whether or not that was cool. But, if I had done something naughty and Amazon had maybe,

revoked my card, you could say, "I'm sorry. Amazon has revoked your card just like browsers now can revoke SSL certificates."

Carl Franklin: Alright, so I got two questions. Number 1, this is all fine for browsing, but these things will work in physical form as well, right?

Scott Hanselman: Right. So more and more they're going to have support for storing this tokens on secured FOBs on, will it be any kind of thing that could potentially provide a more context. So, like...

Carl Franklin: Could you envision a day where you would be able to check in at an airport a lot faster if you have an info card?

Scott Hanselman: If you had like an identity setup on like Alaska Airlines or on United, and you'd associated an information card, if I had that info card on some physical thing and they of course will have to decide whether that was USB or Smart Card or whatever, I could see, whether I would be able to go to a kiosk at an airport and give them this Cert and because it is a real certificate that can identify me as being totally unique and guaranteed to be me and then maybe apply some additional information, because security is not just about what you have, it's about what you know.

Carl Franklin: Right.

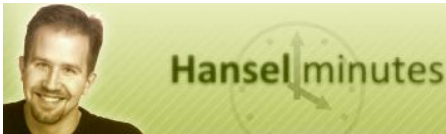
Scott Hanselman: So, the more factors in the authentication, the more legit, that's why ATMs have the card that you require and the pin number

Carl Franklin: ...and the pin. And the second question is, do you foresee of everybody trying to be a card provider just like every business in the world wants you to think of them as the end all be all in all services. You know, what I mean?

Scott Hanselman: Yeah, totally.

Carl Franklin: So, get your Ground Round credit card, get your Mobile credit card, get your Ben and Jerry's credit card. You know, it's like ridiculous and if that's the case, doesn't that sort of defeat the whole purpose of having a universal card?

Scott Hanselman: Yeah, I totally agree with you that having everyone like, your local safe way, grocery store didn't give your card is lame and I know I've got like six different tokens on my key chain.



Carl Franklin: I don't want a 150 tokens and I won't have to...

Scott Hanselman: And I think that the public will make that decision. I think that while there are companies that issue hundreds of different kinds of branded Credit Cards. I know, that I had a Yahoo! card for a while, I think that people eventually, kind of decide that there'll probably be five to ten, the obvious players. If everyone gets up behind this, there will be Google identity, there will be Live.com, Amazon and people will decide that. What really becomes interesting is when Google decides that they'll accept Microsoft Cards and we are not talking about the format, we're talking about the authority to issue them.

Carl Franklin: We shouldn't have to rely on trust relationships between providers in order to have access to things and that's really bothering me. Like I would just want, I would want one provider and I would want everybody to trust it. You know, what I'm saying? I would want American Express to be my provider and I want everybody else to trust it and then I don't have, "Oh! I'm sorry sir, you can't stay at this hotel, because we don't have a relationship with Google or whatever."

Scott Hanselman: Sure, but that's a part of reality though. I don't like going to, like Costco You know, Costco -- the big wholesaler, didn't take debit cards for the longest time. They didn't take Visa, they didn't take MasterCard, they only took American Express.

Carl Franklin: Yeah.

Scott Hanselman: That's just part of business. I think, that same problem is going to happen within the CardSpace spaces, that people would just decide that, "We won't accept this certain kind of card." But I think that the pressure from the public will refer for a clean approach to identity, will eventually make sure that everyone decides...

Carl Franklin: Yeah, and it's going to have to I mean like ATMs, you've got -- how many networks are there for ATMs, but every ATM machine recognizes all of those networks. But, there is only a handful of them. Right?

Scott Hanselman: Well, but every once in a while though you get penalized in some way. I hope you don't get to that.

Carl Franklin: Yeah, I really hope that this works out, so that the consumer wins and not -- it doesn't become a battle for their mind and, -- heart and mind of the consumer.

Scott Hanselman: At this point I don't think that will happen, -- but a lot -- but no managed services have come out yet. Right? I mean, there is not a whole run or rush due to -- to come with your own managed token service.

Carl Franklin: Right

Scott Hanselman: I think, it's going to be probably this time next year, but, the hardware, the software will all be ready by then. I mean Microsoft's implementation of it is just the first step. It's getting everyone else to get stoked about it, right? If it's just the thing that works in Vista, that's not going to be cool. So like now it works in Windows 2003, it works in XP, if you've got .Net Framework 3.0. If people are able to download a tiny certificate acceptor within Firefox, giving alternative browsers, the ability to do this kind of stuff, then it's going to become a lot more palatable. And interestingly I really think it's going to be the blogs, it's funny. I mean just the fact that Kim Cameron's got a PHP one that Kevin Hammond put together a DasBlog win and just today set it up so to work in 1.1 or 2.0 with a Pluggable Identity Provider. Isn't it funny how the people who have no money and run blogs are the ones that do these things first? And then the people with lots of money like Amazon or Google will do it later.

Carl Franklin: Yeah interesting.

Scott Hanselman: It's definitely going to change the game though and I think for banking and for protecting your identity, it's going to be invaluable, for my industry it's going to be fantastic. It's just going to be figuring out what the easiest way to get grandma to run an information card is.

Carl Franklin: So, what's a extended validation?

Scott Hanselman: So, on EV SSL is a kind of certificate that I blogged about recently and you can see that at shrinkster/jkx and this talks about the kind of the evolution of SSL certificates and how -- right now if I visit Franklins.net and I see a little lock up there because I am under SSL. Right there, that lock says the information is encrypted on the wire but people have started to associate that lock with a sense of trust that oh if I see the lock, it's okay. But that doesn't necessarily imply I am looking at franklins.net. I could be looking at Franklinsevilphisher.net. So, EVS SSL is a new kind of extended validation or what they call High Assurance SSL certificate. And these certificates are a new kind of certificates that emerging standard will see it, probably be ratified in the next couple of months. It's supported in IE 7. Now there is an example, you can go and



download it. And you can see it at woodgrovebank.net and basically and if you visit a site that has one of these extended validation certificates, your address bar is going to turn bright green and you are going to get an additional lock that's going to shift back and forth between the name of the organization not the URL but the actual name of the organization that certificate is for and then the certificate issuer and it will kind of cycle back and forth.

Carl Franklin: That's at woodgrovebank.com by the way.

Scott Hanselman: Is it?

Carl Franklin: Yeah.

Scott Hanselman: Oh my bad, hang on one second. Yeah you are absolutely right, it's woodgrovebank.com and if you have installed the test certificate, you will see in IE 7 that address bar turn bright green. It's just an example of what the certificate experience will look like. And what that means to like a bank or any kind of an e-commerce site is that they're going to have to go through some additional auditing to prove that they are in fact who they say they are because like I just got a certificate for hanselman.com from godaddy.com. I think it took, I don't know ten minutes to get an SSL certificate hooked up. It was crazy, I just went up, got the cert, asked my ISP for a request, confirmed that I in fact own the domain and I had a cert.

Carl Franklin: I use instantssl.com, 30 bucks.

Scott Hanselman: Yeah so I mean it's easy to get secure wire access but they want to make it more difficult to say that I am in fact Woodgrove bank or Hanselman bank and I think that within a year or two, we are going to see all of the different browsers supporting that. Firefox has indicated that they will support it, Opera has indicated that they will support it.

Carl Franklin: Usually they are using -- right now they are using like Dun & Bradstreet. You have to have a D&B account and that's an easy way for them to verify your address and all that blah, blah blah...

Scott Hanselman: Right. They want to prove that you are a real organization.

Carl Franklin: Some actually -- they used to come out to your site and take pictures. Did you know that?

Scott Hanselman: Did they?

Carl Franklin: Yeah.

Scott Hanselman: Like auditing?

Carl Franklin: Yeah, they used to require that they would have to come out and take a photo to make sure you are who you will say you are.

Scott Hanselman: Now see some people think that it's not fair to the little guy. They are saying that that's going to make it more difficult for the little guy to...

Carl Franklin: Well, they don't do that anymore.

Scott Hanselman: Yeah?

Carl Franklin: Yeah.

Scott Hanselman: So there is a number of different things that people should be checking out, if they want to learn about Info card, there is a great video up on channel 9 at shrinkster.com/jkw and they can also learn about protecting your identity online. There is a good kind of things that you can do and bits of information about yourself that are low, medium and high sensitivity at shrinkster/jkt and then you can also like I said learn about EVSSL at my blog at shrinkster/jkx. And a lot of people have been commenting that they think this is a way for the certificate authorities to get rich by requiring an expensive certificate and I am not sure whether I think that's the case but there is a good conversation going on in the comments up on the blog there so check that out. I reason that EV SSL makes sense in the context of InfoCard is that both of these things are giving an entirely new visual cue and visual metaphor for what it means to visit a secured site. So there's going to become kind of an expectation on the part of the users that just as they look for that lock, they are going to start looking for that InfoCard, they are going to start looking for that bright green address bar and that new warning, whether or not a site is secure and I think it's conceivable that there will be a time when browsers will come with a default that will only allow certificates that are of this higher assurance. So, not something that's going to happen tomorrow but it will definitely happen in the next year or so I think.

Carl Franklin: Awesome. Well hey Scott, that's a show. Thanks a lot. What a great show!

Scott Hanselman: Thank you.

Carl Franklin: I don't know what else to say about it. It's a great topic and I can't wait to see it evolve.



Scott Hanselman: Yeah, I really encourage people to check it out; go install the .NET Framework 3.0. I am running the September CTP but you can also get the RC1. September CTP is a little bit newer but you can check all of the stuff all about CardSpace at shrinkster/jkg up at Netfx3.com and we'll have all these links up on the Hanselminutes site.

Carl Franklin: All right and until then we'll see you next week on Hanselminutes.

(Music)