



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
January 12, 2015**

Presentation

Operator

All lines are bridged.

Michelle Consolazio, MPH – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology

Thank you. Good morning everyone, or good afternoon I should say; this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT Standards Committee's Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, please state your name before speaking as this meeting is being transcribed and recorded. I'll now take roll. Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Lisa. Dixie Baker? Aaron Miri?

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Good morning.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Brian Freedman?

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Brian.

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Hello.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Jason Taule?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Good morning, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Jason. Jeff Brandt?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hello, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Jeff. John Hummel?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, John. Lee Jones? Paul Clip? Peter Kaufman?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Peter. Scott Rea? Sharon Terry? Steven Lane? And from ONC do we have Julie Chua?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

And Jeremy Maxwell?

Jeremy Maxwell, PhD – IT Security Specialist – Office of the National Coordinator for Health Information Technology

I'm here

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Jeremy. And with that, I'll turn it back to you Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you, Michelle. This is Lisa Gallagher from HIMSS; I am the Co-Chair of the Transport and Security Standards Workgroup and I just wanted to let everyone know at the beginning that I am subbing for Dr. Dixie Baker, who is our Chair; she had an unavoidable conflict today. So I want to welcome everyone, I want to say thank you to the ONC and MITRE support staff, who have been immensely helpful to me. Members of this workgroup thank you for your work with us and also welcome and thank you to the members of the public.

I'd like to go ahead and review the agenda for today and then we'll get started. So today our objective is stated on the agenda slides; we're going to be taking a look at RESTful API security recommendations, that's sort of our generic objective description and we'll talk a little bit more about what we're aiming at. We're going to hear a recap of the presentation that we had last meeting on OAuth and OpenID Connect risks and vulnerabilities. That recap is going to be provided by Mark Russell from MITRE, who actually provided us with the original briefing at our last meeting.

And I also want to mention for the workgroup members and members of the public that in addition to the slides for today, which will contain a recap or a shorter version of that presentation, the full presentation from the last meeting is also posted on our website for reference, or easy reference, today and in the future; but Mark's going to give us a summary. And then we're going to jump into a discussion among the workgroup members on formulating our recommendations that would be provided to the Architecture, Services and APIs Workgroup.

A little bit of background; Dixie and I had the opportunity to talk to the Architecture, Services & API Workgroup's Chairs last week, so that we could talk about the work that we're going to do and the kind of recommendations that might be beneficial for the ASA Workgroup. So, we explained that in building on our work on user authentication around provider authentication that we finalized last month, we...our next task is going to offer us the opportunity to make further recommendations in the areas of two technology...new, emerging technologies, OAuth 2.0 and OpenID Connect, as it relates to RESTful API security.

In talking over that plan with the ASA Workgroup, they thought that it would be beneficial for them to get that input from us as they begin their work. And so also given our recent discussion and recommendation to further assist with the new work that NIST is going to be doing around 800-63, our discussion today regarding some recommended topics to consider will align nicely with the work that we see them doing and our work on transport security federation topics.

So also one other point as we start this discussion is Dixie and I went through our planning for this meeting, we tried to make sure that when we have our discussion at the end of Mark's briefing that we will scope it tightly to the kind of recommendation we want to make and the information we want to provide about OAuth 2.0 and OpenID Connect. But that in general, we are recognizing that there are other recommendation topics that we can consider adding that really have to do with just existing good cybersecurity hygiene standards across the transport infrastructure and other secure coding practices, for example, relating to the HIT environment in general and RESTful APIs.

So they would address common vulnerabilities and attack methods not limited to things like serialization format attacks, cross-site scripting, cross-site forgery requests, sequel injections, etcetera, just to give a few examples. So we will focus in on, you know, the OAuth 2.0 and OpenID Connect recommendations, but we are not...we are mindful that we will also consider referencing just in general our guidance to keep good security practices in mind.

So with that, and again, after Mark's presentation we'll go over specifically the kinds of recommendations that we're aiming at and open our discussion, but I'd like to turn it over to Mark, Mark Russell from MITRE, to give us a recap of the presentation he provided to us on December 3, "OAuth and OpenID Connect, Risks and Vulnerabilities." Mark?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay, thanks a lot Lisa. I think the scope you just gave is very valuable; the stuff we're talking about is important but not all encompassing so those other things are certainly important. If you go ahead to the next slide, sorry, one more. So, just to give a recap of why we're here talking about this; we had done some work for the US Department of Veterans Affairs regarding how to secure RESTful interfaces. The VA has a long history of using SOAP to secure APIs and data interchanges with partners so there were a lot of questions around moving to a RESTful style, which brings a lot of benefits in terms of lightweight support for Web and Mobile clients, but how to get to the same level of security or to raise the level of security to a point where it would be acceptable for VA medical use cases.

So our goal was to write some profiles to help secure RESTful interfaces in a way that was secure and compliant with VAs requirements that would use open standards and that could support the lightweight integrations that the VA will need to support. We are...we have recently wrapped up a pilot implementation demonstrating the profiles and there's a lot of information available on the site if you're interested in that. But with that, I'll dive into the recap of the presentation we gave in December.

So over on the right you can see very small diagrams that are full-size in the original deck of how OAuth and OpenID Connect, the message flows that occur between the different parties involved. So just to recap, at a high level OAuth is what's called an authorization delegation protocol. It enables a user who has access to some web service to delegate that access to a piece of software and do so in a secure manner that does not require the user to provide their credentials to the client. This is done through tokenization, which is a term that's been thrown around a lot lately with Apple's Apple Pay; but

essentially it means the use of a token in place of something like a real credential which has a lot of security advantages.

OpenID Connect, on the other hand, is for federated authentication. So, to enable cross-domain authentication if one organization wishes to allow users from another organization to access their systems, they can do so by logging on to an identity provider local to their organization and OpenID Connect in a similar way to SAML, which you might be familiar with, would provide a secure way for the receiving end to validate that that user has authenticated and that they have certain attributes as attested by the identity provider. So we came in December and we gave a talk about risks and vulnerabilities to...that you might face when adopting these technologies to secure a RESTful API. Next slide, please.

So this is a sort of a cheat sheet of open standards for REST security. I won't go through all of these; our focus was mainly on OAuth and OpenID Connect in part because they are relatively new technologies. TLS everyone is familiar with but also we discussed a good bit about the JOSE standard on the bottom right, which basically brings to JSON the same kind of data level security and message level security that you have with XML Signature and Encryption.

And then at the very top you'll see User Managed Access; this is a newer protocol which shows a lot of potential for dealing with things like patient consent issues and enabling people to set policy-based access in a cross-domain way on their data. So, there's a lot of interest in that. We decided to tackle OAuth and OpenID Connect because they were already finalized standards when we began whereas UMA is still going through the draft phase, but certainly firming up as we speak. Could you go to the next slide, please?

So in terms of OAuth, this is a short list of the...sort of the high points of what kinds of attacks and vulnerabilities exist and what countermeasures are available to counteract them. So, as with any network protocol, in OAuth we have to authenticate the user at some point. They're going to use a credential and in most use cases involving the public, this is going to be a password. So at some point they're going to have to authenticate to an identity provider. They may have some stronger authentication mechanism, but it will often be a password.

And there are also other pieces of data that are passed around in the exchange. There's what's called an authorization code and there's an access token, which convey the user's authorization and the client's authorization to access the data. So as with all these things, they need to be protected in transit and TLS is a very well established protocol for doing that.

The second one, as with...once again, these are all common...many of these are common problems with any network system, but impersonating the server either to get the user's credentials or to intercept access tokens. There are a lot of lower level networking attacks that people try to do to accomplish this and TLS serve authentication is a countermeasure for enabling the client or the user's browser, as the case may be, to authenticate the identity of the server they're talking to.

Manufacturing or modifying tokens; this can be a problem if the token is guessable or is not a long, random enough value. One approach to this that's taken by OpenID Connect, and which we recommend for all OAuth implementations, is to use signed "JOTs," excuse me, JWTs as the tokens so the signature proves the authenticity of the token and also prevents it from being modified and the chances of being able to generate a fake token with a valid signature is vanishingly small. So...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

I'm sorry to interrupt; I'm trying to save questions until the end, but what is a JWT?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

I'm sorry, that's JSON Web Token, it's...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Okay.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

...it's a token in JSON format that is signed using JSON Web Signature, so it's similar in some respects to a SAML token, it's basically something that's been signed by the server that would contain claims about either the user or an authentication event that's happened.

Justin Richer, MS – Principal Technologist – MITRE Corporation

Right, and I wanted to interject...this is Justin, that we are also in our profiles, requiring things like expiration, issuance time and a random string called a JWT token identifier and with sufficient entropy in them. All of these added together and protected by the signature make for an unguessable and unmanufacturable without access to the private key token.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Thank you, Justin. So, does that answer the question? Okay...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Yes it did thanks a lot.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay, sure. So OAuth requires redirection to sort of orchestrate the conversation among the different parties in the transaction. So one of the risks is that if a client or a browser is redirected to the wrong place, secrets might be exposed to the...to an unintended party. A lot of this can be locked down through things that are optional in the stack, but you can require all clients, when they register, to explicitly state what URIs they're using. This prevents a lot of attacks where the attacker might try to change the URI to which a client would be redirected.

There are also client credentials involved in OAuth so as with any credentials, they need to be protected. One of the things we're recommending, once again, is the use of signed JWTs for clients to authenticate and this basically...a lot of existing implementations use what amounts to a long password for client credentials. By switching to JWT client authentication, the client instead sends a signed message to the server to authenticate. So the private key used to generate that message is never actually exposed to the network provides for much stronger authentication of clients.

And then finally, client session hijacking or fixation; so one of the big challenges in the design of OAuth is that you have two separate sessions going on. You have the user in their browser talking to the authorization server and then you have the client, at some point, directly talking to the authorization server and the resource server. So tying all this together and making sure that you have one unbroken session, where no one has gotten in the middle of it and substituted one session for another is critical to ensuring the security of the whole transaction. And fortunately the spec does provide a parameter for doing this called the State parameter. This basically ensures that, as I said, there's a single authorization

flow and that you're not associating an authorization code with the wrong session or something along those lines.

So a lot of these countermeasures are in the spec, many of them are optional. And so by standardizing on some of these improvements to what you might call the baseline security of OAuth, you can really improve things quite a bit. The key is that there has to be agreement among the community that's interacting with each other to standardize on these specific countermeasures being in place. And the other big benefit to doing that is you have a high guarantee of interoperability among all the parties using the same profile. If you go to the next slide, please.

So as I was just mentioning, so we wrote profiles for OAuth that recommend most of what's on...or excuse me, all of what's on the previous page. There's a bit more to it than that but basically by making a few key changes things are significantly improved. Client authentication with JWT makes for much stronger assurance that the client you're talking to is the one you think you're talking to. Tokens as JWTs means that you could have relatively easy validation when you receive a token need to know whether it's good or not. It eliminates the risk of brute-force threats and then the redirect, requiring clients to register their redirect URLs nails down a lot of the issues with people trying to direct authorization codes or tokens to the wrong place. So I think those may be the three high points of improvements you can make to OAuth as the minimum level of OAuth that's specified in the OAuth spec.

One of our additional requests from the VA was to think about what are some other things you could do to further enhance security for use cases where maybe some impact to usability is justified; you have specifically sensitive API that calls for higher level security, what can you do in those cases? So included in the spec is the possibility of TLS client authentication; instead of using a JWT you could use mutual TLS authentication. And then there's a set of draft specifications for proof of possession tokens which would provide something along the lines of "holder of key," which would provide even stronger authentication. So those are in the spec and those are some sort of enhancements you can have even above what we've specified in the profile. Can you move on to the next slide?

So, moving on to OpenID Connect; OpenID Connect is built on OAuth, so it sort of implicitly inherits all the same considerations. The roles of some of the players are somewhat changed, but if you look at the OAuth...the OpenID Connect flow, it is an OAuth flow. One of the main differences is that the identity provider...excuse me, the protected resource that's being protected is identity information about the user; so, once the OAuth flow has been completed and the user authorizes a relying party to get their identity information, then there's an OAuth token that's used for that access.

So, the authorization server or identity provider can also issue what's called an ID token which is a JWT or "JOT" containing identity and attribute claims about the user. UserInfo Endpoint is a new protected resource where the relying party can request additional claims if something that's needed is not in the ID Token. And the use of OAuth scopes controls which attributes are being requested. So if you're familiar with SAML, this is conceptually very similar.

And so essentially a lot of the risks and countermeasures are the same as what we discussed with OAuth. A couple of additional considerations for OpenID Connect is that obviously the relying party is placing significant trust in the OpenID provider, if some of those claims about the user control access, something like is a licensed medical practitioner could be a user claim. And this is not a new issue, this is sort of inherent to identity federation, but it is something to think about. And finally, if a token is intercepted or manipulated, it could enable a user to impersonate other users. And once again there are

some countermeasures in the spec that help mitigate this, defined JWTs means they cannot be modified or that modification would cause the JWT to not be validated successfully.

And then there's something called c hash, which essentially ties together the authorization code with the token in a somewhat similar way to the State parameter, to make sure that there's been no substitution during the actual authorization flow for the OpenID Connect authentication. And then...I'm not sure if that's my last slide...if you go ahead one more.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I think it is, Mark.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay. Okay, so I don't know if you want to open it up for questions or...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, let's open it up for questions before we move on to our discussion about our recommendations. Also I want to let the workgroup members know that Mark...Mark Russell and Justin Richer will both be on the remainder of the call to help us with any further background or depth that we need, in terms of questions on their presentation. So, they'll be around for the rest of the meeting; but any questions for Mark at this point?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Yeah, this is Peter Kaufman again, sorry to interrupt you before with the question about JWT. Are the JWT tokens hard tokens or soft tokens on a phone or are they soft tokens that would be stored on a computer?

Justin Richer, MS – Principal Technologist – MITRE Corporation

This is Justin; I'll take this. It's...a token is, unfortunately overloaded in many different ways. This is not token in the NIST 800-63 sense in that it's a second factor of authentication token. This is token in the sense of a software security token as in something that is passed across the network that either contains directly or allows referential access to a set of security and authorization information or identity information in some cases, like with the ID...so this is...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

So it would be a token that could be triggered by something like a NIST 800-63 token or it could not be it could just be a user password and username.

Justin Richer, MS – Principal Technologist – MITRE Corporation

That's correct. So Mark mentioned this in passing, the...both OAuth and OpenID Connect don't specify directly what the primary authentication of the end user to the authorization server is...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Yeah.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...that's something that other sets of policy and NSTIC is, for example, trying to get into specifying some of that and...but, as far as OAuth and OpenID Connect are concerned, somebody has to log in somehow. Now we do go, with our profiles we do go beyond that and specify that with OpenID Connect, when you're actually doing an identity transaction, you do have to carry the...what's called the authentication context reference with the ID Token so that will contain a URI that references the user used a hard token to log in; they used a certificate to log in to the identity provider...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Yeah...

Justin Richer, MS – Principal Technologist – MITRE Corporation

...but also...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

I think it would be great to have like...for somebody to do a 5-minute walk through to say, okay, here I am, I'm taking my username and password and putting in my one-time password or my CryptoKey and then say, and the computer's generating this JWT and here, you know, the JWT that's generated because the person logged in and identified themselves and it goes in and OAuth does this. And kind of rather than doing it at such a high level like we've had in these talks, it's hard for me to follow and I think I'm probably more in tune with this than the vast population, but certainly less in tune with this than you other security guys and I'd like to try to get more on the same page if somebody would be willing to do something like that, just so I could get more of an image of what's happening.

Justin Richer, MS – Principal Technologist – MITRE Corporation

I would be happy to and I can actually give a 60-second overview on this call if our Chair is willing to go that route.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

No, I think that's fine. Is that Justin?

Justin Richer, MS – Principal Technologist – MITRE Corporation

Yes, this is Justin.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, Justin, I think that would be fine.

Justin Richer, MS – Principal Technologist – MITRE Corporation

All right, so in that case, if we could flip the slides back to the one with the two diagrams on the right-hand side, I think it was slide 4...one more, try slide 3. There we go. All right, I'm going to be talking to these diagrams and since you can't see me waving and gesticulating, I'll try to be clear about which bit I'm talking about.

First you'll note that both OAuth and OpenID Connect, the diagrams look pretty much the same and that's because they are built on the same fundamentals. I'll specifically be referencing the OpenID Connect diagram down at the bottom and talking about the user identity case and with the...because

there are more JWTs and things that actually come into play there; but with the OAuth case where you're delegating authorization and a lot actually...there's a lot of overlap between those. I'll also state that I'm going to be talking about one of the more common and slightly more complex versions of OAuth and OpenID Connect which is called the authorization code flow.

So with that, if you look in the lower left-hand diagram, you see there's a person with a web browser, the end user and user agent, to use the terms of art. We're going to start there. They're going to be going to the relying party, which is the site that you're ultimately trying to log into, the thing that you're trying to give your identity to, with their web browser. Now this does also work with native applications, but we're going to just have a web-based relying party site for now, for simplicity sake. If you're interested in the deltas and the details, we can probably take that conversation offline. Now...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Would this be visible on the web page or would this be behind the scenes on the web page, the relying party actually being the web page host or would it be somebody that the web page host is logged into?

Justin Richer, MS – Principal Technologist – MITRE Corporation

It would be...it would most likely be the web page itself...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Okay.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...so if you've ever been to a website that says, click here to log in with Google...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Yeah.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...you're actually doing OpenID Connect there; it's just an OpenID Connect that's been branded with Google's end user experience. So, I'll very quickly go through kind of what the moving parts are and at the interest of not derailing the whole conversation with a deep technical discussion. I'll try to keep it relatively high level, but deeper than what we had before.

So the end user shows up at the relying party, that creates one session...one web session there. And the end user indicates to the relying party through some mechanism that they have an identity provider off somewhere else. So at that point the relying party then actually sends an HTTP redirect, an HTTP 302 found code, to the user's web browser that sends them over to their identity provider. At this point, that user's browser creates a web session with their identity provider...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Like Google.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...yeah, like Google, exactly...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Um hmm.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...or the VA for somebody with a VA account or any number of things. So at that point you've got a session over there. The redirect has a bunch of query parameters on it that are passed through the browser, including an identifier that identifies the relying party that you're coming from, the rights of access...the scope parameter which tells you the rights of access that the relying party wants and that State parameter which is a session fixation security component that Mark mentioned before. And there are a couple of others that are less important.

So you show up with all of those parameters and that tells the identity provider kind of what's about to happen here; I mean, somebody is trying to log you in when it sees all of those parameters at what's called the authorization endpoint, which is the little blue AE box. And apologies to everybody for the diagrams being shrunken in, we weren't expecting to do a deep dive.

At this point the end user actually needs to log in with their identity provider. This is where the best application of your multiple factors, your certificates, your hard tokens, anything that would be considered a primary credential would be applied. Because all of this can be well known and well bound by the identity provider. So you show up and you type in your password or you give your one time pad or you present your certificates or whatever is necessary to authenticate the end user with that identity provider.

Now note this is very important to the flow of the protocol that all of this is passing over that connection between the end user and the identity provider and none of that is shown to the relying party. All of that is shown to the identity provider. At this point the identity provider knows who you are and who's asking for the right to log you in.

So the identity provider will classically prompt the user and say, hi, it looks like this site is trying to log you in, here's the information that I have about them, here's what they're asking for, here's where they're going to be sending you when we're done here; does that look okay to you? End user, please make a decision. This is, of course, a place where systems administrators can also whitelist sites or blacklist sites or set things up so that different flows can actually happen here, all using the same protocol base. And that's important with a large scale enterprise deployment, which is where we've been seeing a lot of uptake in OpenID Connect.

Now, at this point the authorization server knows who you are, it knows the authorization decision that's been made. It knows who is being authorized and what they're authorized for. It mints a one-time use, limited lifetime special code called the authorization code. That authorization code gets tacked onto a URL and called the redirect URI, which is hosted back at the relying party, back at the client we're ultimately trying to log into. So that is sent as another HTTP redirect, through the browser, back to the client.

So the user here has done all of their authorization with the identity provider and then they effectively get handed a URI that says yeah, you're done here, go over here now. When that lands back at the relying party, it can pluck that code off of the redirect URI, along with the State parameter and a couple of other things so it knows that this is the response to the request that it made a few moments ago and it can then continue the transaction. Now remember, right at the very beginning the user started a session with that relying party, so we know that it's coming back on this session where we had generated the State, we're getting back this code, we're great. We still don't know who you are and nobody's actually logged into the relying party yet though, so there are a couple more steps.

The next step is for the relying party to trade that token in a direct HTTP call, what's called the token endpoint over at the identity provider. Now this is authenticated with the client's credentials, not the end users credentials; but in that first redirect the client...the relying party had sent its identifier. Now the client sends not only its identifier, but also, using our profiles, a signed assertion of its identity that is backed by its own registered public and private key pair and signed by its private key.

The authorization server can then verify that, because this client has registered with its public key and pairing that public key with a specific client identifier at this server. It can check the signature on that assertion and verify that and it can also know that this code was, in fact, issued to that particular client identity for a certain set of rights, in the context of a certain user being authenticated.

So you can see here we have closed all three legs of this triangle and the authorization server can collapse all of those together and say, this user, this client, this set of information at this time, with this context all exist within this set of tokens. This is where the JWTs come into play. In OpenID Connect, you get issued at least two; the first is the identity token or ID token. This is a signed JWT that has information about the security context and basic information about the end user.

That is meant to be parsed by the relying party directly; so it looks inside there, checks the signature and makes sure it matches the server's published public key now and makes sure that all of the expirations and everything lines up. That includes information about a very basic identifier for who the user is called the subject. It's analogous to a SAML subject as well. And that's no mistake that those line up.

Now at this point you've got the ID token that tells you basically who showed up, but it doesn't really tell you any information about them like what's their email address? What should I call them instead of user AB346? That's where this next step comes in, where you have what's called the access token, which is another token that's issued alongside the identity token. That can be used when necessary to call what's known as the user information endpoint, which is effectively a profile endpoint that has that information such as the user's name, their email address, their physical address, phone number, other bits of information that they might have. And the user, in most cases, is able to determine which bits of information they actually want to release to a particular relying party.

So unlike a certificate where it's everything is baked into a certificate and it's all or nothing and you have to disclose that just by the nature of using the certificate; but using these tokens we can actually pare down the information and give end users control over what's passed at every step.

Now the last bit of information here is that OpenID Connect and OAuth out of the box don't say what that token looks like; it could be a random BLOB, it could be XML, it could be JSON, it could be a binary thing; it doesn't...OAuth and OpenID Connect don't care. The profiles that we've written actually specify what that token format is and we are reusing JSON...signed JSON Web Tokens with a couple of key pieces of information inside of them. That allows us for a better baseline security and greater interoperability between different what are called protected resources, which is more useful in the OAuth...in the generic OAuth case where you're protecting perhaps a bunch of different APIs from different vendors and a particular authorization server for a given user.

So the JWTs really come at the end of that whole process of setting everything up and the protocol is designed in such a way that there is limited information that is passed along every single link.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So Peter, this is Lisa; does that answer some of your questions around...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

It answers a lot of them.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

...okay.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

One more question and that is, when I've signed on to web sites that say, sign on with Google, which I don't usually do, but if I do sign on with Google, it doesn't ask me to sign on with Google the next time I go to that web site. Does it keep that token as a cookie or something of that nature or...and for healthcare, are we talking about having them sign on using the OpenID Connect every time they sign on or are we talking about delivering something to the computer that will authenticate them in the future?

Justin Richer, MS – Principal Technologist – MITRE Corporation

So that's actually a very complex question of web session management. In your case, they probably are storing, in your anecdotal example, they probably are storing a long term cookie.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Um hmm.

Justin Richer, MS – Principal Technologist – MITRE Corporation

You would probably want to have a wider set of guidelines about local session lifetimes, which will, of course, be kind of application specific, but it's good to have guidelines for things like that, too. Because at the end of the day, you're not going to because at the end of the day, you're not going to have somebody go through an OpenID Connect transaction for every single page-load; you're going to want to tie them to a session of some type. But when that session actually winds down, that's up to the relying party, the site you're ultimately logging into.

That said, if you know that the person that is in that browser used a particular identity provider last time, you can actually short circuit the beginning of the process by just guessing, as a relying party, and it really is a guess at this point; well, you logged in with this place last time, I'm just going to try to log you in using that same identity provider last time and if you already have a session over there and I'm already authorized to log you in, then all of that happens very smoothly and transparently to the user without the need for a long term security token. So you're still getting a fresh session, but you can store hints as to kind of where you should go.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Great; thank you very much, this was...it was really very helpful to see this.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Great. Okay, any other questions at this point in time for Mark or Justin on Mark's presentation? We are going to, you know, taking that information look at, on the next slide, a list of some straw

recommendations and they will still be around for that discussion. But I just want to pause one more time to see if there are any further questions at this point.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Yeah Lisa, this is Jason Taule. I do...it's not so much a question as an observation and one I'd like Mark and Justin just to comment on for our benefit. I think it's important to understand the context in which this technology is being considered. Based on the explanation that we just got clarification on, I think it's very useful for the exchange and the trust that we can have in relying on an identity proven previously for a current or future use case. That doesn't necessarily mean...this says nothing about the legitimacy of the identity when...that's currently on store with the OpenID provider.

So if I go to Google and I create an identity claiming Lisa Gallagher and I provide Google with credentials and I have an identity and then I go in to log into another site having hit request information from a fake identity that I've created, it's going to do the exchange very properly, very securely with limited risk, but that doesn't mean the original registration was legitimate. Right, so this is only as good as whatever faith we have in that original registration. So that's just an observation. I want to get their reaction to that.

Justin Richer, MS – Principal Technologist – MITRE Corporation

This is Justin; I'll take that because this is actually one of my favorite topics lately. So, you are spot on and there are actually a few different things in play here. The first is what you would generally term identity proofing, so how sure are you about a particular set of attributes? So, you or I could go and as far as Google's concerned, we self-assert to be Lisa Gallagher and Google doesn't care what you call yourself, they just want to have a name there. That's one set of attributes.

However, there are a couple of other things in play here. The second is the strength of the credential that binds a particular user to a particular account. So no matter what name your account says, if you've got multifactor authentication and heuristic authentication and other things that are all tying you to that account, whether or not it claims to be Lisa Gallagher, we can be pretty sure that it's the same person, you know, modulo beating the password out of somebody with a wrench but that's another story.

We can do a lot of stuff with these very strongly bound pseudonymous type of accounts because at the far end, it's not actually looking at the username or the display name of Lisa Gallagher or a particular email address in order to get you into things like say a particular medical record. You have to be able to bind...with a system like this, you have to be able to bind a given account identifier regardless of what the other attributes say, to a particular set of rights including the right to access a given medical record.

Now the way that I personally think that this technology needs to go is for at least the happy path, we need to be able to allow people to take a pseudonymously bound account with a strong credential set and possibly zero identity proofing ahead of time; they need to be able to bind that in a strong way to a particular medical record. So take for a concrete example I walk into my doctor's office. My doctor knows me and he pulls up my record while I am sitting there in the office. And my doctor has a lot of assurance that I am a particular patient and they have the right record there for me. If I can then, in that moment, demonstrate control over a given digital identity, it doesn't actually matter if that digital identity has Lisa Gallagher's name on it, because they're not using that to look up my medical record, they're using the unique subject identifier, which is a non-human readable BLOB in most implementations of the protocol, that is meant to be stable for a given account over time regardless of

whether or not all of the rest of the attributes change. So we can do a lot to strongly bind that particular thing.

Now there are, of course, other aspects here like how much do I even trust a given identity provider? Has a third party independently come in and assess the fact that they onboard people and they don't just publish their passwords on a website. You know, they claim to do two factor but do they actually do two factor? All of that's where trust framework providers and things like the Kantara Initiative, Open Identity Exchange and other things like that can really come into play as trust framework providers and make those independent assessments and then you're buying into a particular trust mark.

All of these different things, including also sort of the operational management of the identity provider and the relying party and other players in this landscape including attribute providers and what not; all of this has classically, with the NIST 800-63 Special Publication, been boiled down into a single level of assurance number. The thinking now is that that is...that's too coarse of a grouping so there's a lot of work that's being done currently to kind of separate out those different aspects. One which I'm personally involved in, and we are welcoming people to the conversation, is called Vectors of Trust in...and that's a conversation that's taking place in the IETF, Internet Engineering Task Force.

So if you Google IETF Vectors of Trust, you should find our mailing list and if you're interested in helping figure out how and where we split apart these different aspects of identity proofing versus credential presentment versus the strength of the assertion as it crosses the wire with all of the bits and JWTs and things floating around, please join the conversation. NIST, I am aware, is also looking to sort of write the next generation of 800-63 and perhaps NB-404 as well that help us talk about this in a more standard way across different security domains. Great question.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Thanks, thanks. So, to the next point, Lisa, I think when we make rec...when we talk about the recommendations, it's important to recognize that this is but...it's a very important technology but I think it's one component of a larger solution where we need to yet identify what some of those other pieces would be.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I think that's right and I think as we consider our next areas of focus, we can take a look at that, I mean, I think that's right. And we've already had a presentation from NIST on 800-63 and their thoughts about this going forward. And in terms of NSTIC, they use the terminology componentizing trust and expressing those in terms of trust marks. And here with IETF, you use the terminology vectors of trust, but I think this is conceptually something that we've been looking at and we need to continue to focus on so that we understand how it can apply in healthcare.

Justi...Jason, was there any other question that you had or further clarification that you'd like to have.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

No that was perfect. Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Any other questions for Mark or Justin at this point?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Jason...this is Jeff Brandt; Jason, what's your last name?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Taule, T-A-U-L-E.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

I see it now, thank you.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

You're welcome.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

And Jason is a member of our workgroup. Okay, so if there are no further questions, I'd like to point our attention to slide 9. Okay, so considering our previous discussions and the recap that we just had today, in the discussion that Dixie and I had with the Architecture, Services and API Workgroup, we, Dixie and I along with ONC and the MITRE staff have taken a stab at some straw recommendations that sort of help us walk through the kinds of things we want to touch on as we consider our advice to the ASA Workgroup, either strictly regarding how to authenticate and authorize RESTful APIs, and our specific focus here on OAuth 2.0 and OpenID Connect.

So I'd like to go through these six sub-bullets. We've also got some examples to help explain them. I'd like to go through those and then open it up for workgroup discussion as to whether these are the right set; if this list is comprehensive, any changes in wording or any other consideration that the workgroup would like to discuss. So, any questions or procedural points before I go through these sub-bullets here?

Okay. So this is the list that we developed, and we did focus on the wording, but we're certainly interested in your feedback. The first bullet, enhance stronger client software authentication by using standardized signed web tokens instead of passwords sent over the net. So we know that passwords by themselves are no longer adequate and the implementation of HIT RESTful APIs is definitely going to require stronger authentication approaches. And this is really why we felt that this recommendation to use standardized signed web tokens instead of passwords was worth mentioning.

The second bullet, recommend that HIT RESTful APIs adopt for use OAuth 2.0 and OpenID Connect standards with TLS encryption. So this is in further support of the bullet number one, first bullet there; RESTful APIs based on our presentation recap that was just had by Mark, we believe they should adopt OAuth 2.0 and OpenID Connect standards with TLS encryption for authentication and authorization, transport federation for software resources. That's sort of connecting to the first bullet.

The next bullet, use of TLS encryption with server side authentication assures the client is communicating with the correct server. The information is also thereby protected across the established link. So when a client connects to a server resource locally or in the Cloud, the initial authentication handshake is just as important to encrypt as the established session between the client and the server for protection of the data as well. So here we're talking about encrypting that initial authentication handshake.

Minimize redirect manipulation risk exposure by using declared redirect Unique Resource Identifiers, which are URIs, during registration. So due to risks in the implementation, this also applies to static and dynamic registrations of URIs.

The next bullet, establish and enhance RESTful API security vulnerability testing to minimize evolving cybersecurity risks. So, you know, this is...our discussion thus far has been around known and documented vulnerabilities; we just want to raise...we thought it would be a good idea to raise the issue of overall risk awareness and risk assessment given the evolving cybersecurity risk and that we should emphasize that security assessment and vulnerability testing has to continue as well, to continue to minimize risk in this scenario.

And the final bullet, ensure appropriate awareness and mitigation of cross-site API vulnerabilities; one example of that is cross-site scripting related to client side web browsing and when we were talking with Justin and Mark or Justin the other day, there are also many other examples related to that, but so ensuring awareness and active mitigation of the vulnerabilities around cross-site scripting and other examples of cross-site API vulnerabilities. So, at this point I'd like to open the discussion on this set of six bulleted recommendations for us to consider forwarding on to the ASA Workgroup.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

This is Aaron Miri; I have a comment. I think these are great recommendations. I just want to throw on the table that, and this might be a little more higher level than going into some of these recommendations but sort of at a high level, at a macro level that we obviously, I work at a pediatric health system and we use one of the major EHR vendors, I'll withhold name. But at this point, they're stuck on Internet Explorer 9 and there's...and other hospital systems are stuck in IE 8 or others, due to the respective EHR that they're using, not yet certifying a more current browser.

And I understand that we're looking at web tokens and TLS and things like that, but I think at a more macro level, is there a way we could recommend that in order to say certified, per se, that it needs to keep up with technology. Because what's happening now is that, from my perspective, my own personal perspective we're having to keep our organization watered down with a browser version that isn't supported anymore simply because our EHR vendor cannot keep up. And this is the same story being played out over numerous providers across the industry. Is there a way at a more macro level we can encourage adoption at a more rapid pace of the more recent technologies in the market?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Umm, Michelle and Julie, this is a question that I have regarding Aaron's comment. We here have agreed to provide recommendations to the ASA Workgroup, but this recommendation I think would be to the Standards Committee or to ONC as far as the Certification Program directly. What are your thoughts about including something like that here?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Hi Lisa, this is Julie. So in consideration of what Aaron just said, there...there are two ways to address that one is when we say that we are sharing our recommendations with the ASA Workgroup, in the end, it would still be a recommendation to the Standards Committee. So whatever recommendations you present to ASA, they either say it's aligned, not aligned, agree or disagree and then we would present that to the bigger, broader committee and that could include some of the recommendations along the certification route. So, we can definitely put in certification recommendations if this workgroup feels that it is something that ONC should look into.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So then Aaron something along the lines of recommend that in order to facilitate the timely use of RESTful APIs include requirements within the certification program to...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

To utilize technology no older...not older than 12 months or something along the lines here, and we can debate that; but just something to reflect the fact that we feel that there should be an urgency level with adoption of technology because, I mean, even Microsoft has begun sun setting old JAVA versions because they just can't keep up with all of it and they're forcing people to be ahead of the time with JAVA. So, why...we should encourage that same type of adoption curve within the marketplace and say look, get with it, certify newer technologies so that people can be secure and utilize things like RESTful APIs.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So any comments or input from the rest of the workgroup members? Is this something that you'd like to include?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel and I'd say yes because currently the hospitals that I work in right now, we have five different EMR vendors that are present and their requirements in terms of staying current with either Microsoft, Firefox or Chrome are scattered across those five. And I think that part of a certification process would have to have some type of language in it that says that just because you can certify to the 2015 version and therefore you don't need to do any more development; you need to keep those vendors where they're staying current on the releases. Of my five vendors right now, three of them are still on XP.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Ick, okay.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Yes, amen to that. This is Aaron; I have the same...I reflect those comments.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

This is Jason Taule again; I think we're right, I think we just want to make sure that, so we anticipate and refute a possible objection on the part of the consumers of these recommendations that we're only talking about the browser. There are many, many healthcare providers that have long term investments in technology where unfortunately they don't have the financials to keep up with everything else; they already have...they've read numerable articles that talk about how running out of data and older, no longer on support technology is not consistent with HIPAA; we're only talking about the browser.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

That's what I was referring to; this is Aaron. Yes.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Right.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So we are referring here to the browser because it is something that could be in the critical path of adoption of RESTful APIs.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Exactly.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Perhaps we could say to the ASA Workgroup, and anything else that you know of that would be prohibitive to the advancement of the use of RESTful APIs. I mean, there may be something else that we don't know about.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Right because...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

...browsers and anything else.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Right and I think where all the EHR vendors are going, especially if you talk to the major players is, leveraging more and more to be browser based versus FAT...based. And so I think we're covering ourselves from a future state by staying along the browser-based path because it will help now and it will help in the future even more.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. So any objections to adding in that kind of a recommendation from our group through to the ASA Workgroup? Okay. Any other thoughts, comments, edits on the list of six bullets that we have here on the slide for our recommendations to the ASA Workgroup?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

So, just one clarification that we might want to make sure we have addressed...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Who is this speaking?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

...this is Jason, my apologies. I think most of us have, when going through that prior step-by-step walk through, we imagined a PC and the user sitting in front of that when encountering the browser.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

That...I don't know that all these technologies and all these recommendations are as applicable...we'd want to make sure that we anticipate the question of, well, are you also saying that that works for a smartphone as well or a tablet or whatever the endpoint the user might have. And I know that there are differences there in terms of capabilities and what the functionality of browsers and things like that is.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Justin or Mark, any thoughts on that?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Yeah, I mean we explicitly were considering mobile clients for our work. There's nothing inherent about it that would be an issue for a typical smartphone; that is one of the advantages of being browser based. When it comes to the actual client that's consuming the API, there might be differences there in terms of the native platform you're writing to, but in terms of the security mechanisms we talked about, smartphones are well supported.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems

Right and...

M

This is...I have something I'd like to say here. Maybe instead of just saying the browser, would we be more...by saying client and then it does...you don't get caught in the browser if tomorrow we change from browsers to something else or if it's a native application which doesn't use the browser at all?

M

That works for me.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, I'm looking at the recommendations and I don't think we use the word browser there.

M

Can we say client, I'm sorry, I hadn't read this but that is more appropriate because one of the browsers is, you know like spreadsheet IE they have a lot of...if you're using ASP or something like that, you can add a lot of the functionality that is...type browser, not really under the standard of...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

That's true although, I mean, I would say maybe you could do both, right, you say browser or client used to deliver the HIT information. I mean I think most future state clients are going HTML 5 and are going to be pretty portable across multiple domains and vehicles. So...but I think that's a fair point to say maybe both, say the browser and/or whatever respective client is delivering the information, that would cover us both angles.

M

I agree.

Justin Richer, MS – Principal Technologist – MITRE Corporation

This is Justin and for what it's worth, I agree as well. I think if you take a longer look at computer software, we keep going back and forth between thin-clients and fat-clients. Right now we're seeing a shift away from direct web access to native mobile applications on smartphones, so that's away from thin to thick and I think we'll go back to thin-clients and back to thick again and again and again. So fundamentally it is a client application of some type, but in order to address the concerns about browsers themselves in the immediate context of this, I think the language of browser or client is appropriate.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. And I have browser or other respective client delivering healthcare information; it's long, but it gives us some context.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas

Right and I think the committees will appreciate that downstream to know that we were thinking of both angles. That was a very good point to pull the other angles into it about mobility because I think that goes right back to the whole point that even the Congress has made about interoperability so this is showing that we're looking at all perspectives.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Agree.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel; can I make a recommendation that we change the wording a little bit for your very last bullet point because I think cross-scripting is a very dangerous, in my mind, when I take a look at like our patient portals and how they're coded and put together, they're fairly vulnerable to that cross-scripting. As we look into the future and we look into these larger Blue Button patient portals, I'd like to have that better emphasized that the programming that goes down the line for certification is really focused on preventing cross-scripting.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. I'm not sure that the Certification Program looks at the actual programming side. Does anyone know the answer to that? But, I mean, there's nothing wrong with passing that on as a recommendation but, I'm not sure they currently do that.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

I know that in the certification process they try to stay away from mandating program techniques or programming languages...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Right.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

...but I think that there could be additional wording in terms of not just awareness of cross-scripting but the mandate to make sure that the...as part of the certification that cross-scripting is tested as part of the jury.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Umm, okay, I see your point. I mean here we are talking about...our recommendation talks about just the general use of OAuth and OpenID Connect.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

Um hmm.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

But here you're saying a recommendation to the Certification Program to consider the risk of cross-scripting and figure out how to deal with that, if possible, through the certification.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

Right. I know that when we first started out with CCHIT and we started writing the first juries, we were kind of implicitly told not to try to get down to a specific level where you're mandating the vendors to do something specific. But I know that when we first started the jury testing for security, we actually

went through the process of saying that here are some vulnerabilities that we need to make sure that you have addressed as part of your certification so we just don't put out bad patient portals, that there's some security built into it. So that's part of the original juries that we did.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Umm...okay. So, I mean, we could make this a little bit more generic and just say that if possible the Certification Program consider certain programming related vulnerabilities such as cross-scripting and figure out if there's a way that they can deal with it in the Certification Program; something along those lines?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

Yeah, I would be good with that.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Any other thoughts or comments from the workgroup members?

M

I mean the other way you could state it, I mean we're just getting into semantics here, right? But I'm not the best wordsmith here, I'm more of the engineer guy but I would say that we could encourage or state that there needs to be some sort of preventative countermeasures built into browsers to prevent cross-scripting or something to that effect, just show sort of a proactive approach that as you're going through and building out say a patient portal, to use the example that was given, that concept and build and test is made with cross-scripting prevention in mind.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Julie, is possible that we can sort of offline work on the exact wording of this recommendation and send it out afterwards? Or do we need to resolve it here?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Uh no, I think we can come up with language first...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

...yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

All right. Thank you, John. Any other...

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

Yeah, this is Aaron, I’m happy to help with that, too if you need anything.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, wonderful. Thank you. Other comments? Edits? Thoughts about the six bullets of recommendations as presented here? Okay, and then we do have one final thought here on the last bullet. We were talking at our last meeting about the HEART Initiative, the OpenID Foundation Health Relationship Trust Working Group and here we are recommending that we as a workgroup consider tracking the development and the piloting activities of that working group as potential standards for privacy and security specification in RESTful HIT APIs going forward. So it would be our own task to track that and at the appropriate time, make recommendations, if applicable, on how they can be incorporated into the use of RESTful APIs in healthcare; thoughts on that recommendation?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel again; I would support that.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yeah, it’s just sort of a reminder for us to continue to track that recomm...to track that activity for potential future recommendations.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

Exactly.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

Yeah, this is Aaron; I would agree, I think it’s worth it.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay.

Justin Richer, MS – Principal Technologist – MITRE Corporation

And this is Justin, just for the benefit of the working group members; the initial phone meeting of the HEART Working Group is actually later on this afternoon...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Oh.

Justin Richer, MS – Principal Technologist – MITRE Corporation

...at 4 p.m. Eastern time. It is open to the public; to contribute anything, you have to agree to the OpenID Foundation’s IPR, which basically means anything you say is considered a contribution to the...a public contribution to the working group; it’s really not onerous. But, for information on that, go to OpenID.net/wg/HEART. Or, if you just Google OpenID HEART, you should get the working group page, which should have the connection information on it. The mailing list is also now open and people can join; so, we are literally seeing the start of this working group like right now.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So Justin, that's the kickoff meeting today.

Justin Richer, MS – Principal Technologist – MITRE Corporation

Yes, the kick-off meeting is this afternoon 4 p.m. Eastern time.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you for that information. Okay, for the working group, any further comments, edits, questions, input on the recommendations on the slide as discussed today? Okay, so Julie, with regard to next steps, I think we...we didn't have any specific rewording for any of the recommendations on the slide, but we did have a couple of additional recommendations that we're going to draft language for; so we can take that, you and Dixie and I, take that as a next step for the workgroup and we can, I hope handle that via email.

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Right.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Your thoughts on that, definitely through email?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Yes and basically what we can do is MITRE and myself, I can share with them my notes, if you had any notes as well and they can come up with draft language. I know that certain people on the workgroup have also said that they would be happy to provide input and we can take all those, put together the draft recommendations again and we can send it out to the group for review prior to the next meeting on January 28.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, and as far as approval of those additional recommendations, would we handle that via email or at the next meeting?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

Umm, I would say at the next meeting so that it is public record.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Any other next steps that you want to discuss for the workgroup Julie?

Julie Anne Chua, PMP, CAP, CISSP - Information Security Specialist, Office of the Chief Privacy Officer – Office of the National Coordinator for Health Information Technology – Department of Health and Human Services

I don't think so and I am sending you, Lisa, a link or an email with the HEART Workgroup information and you can send it out to the rest of the members. Thank you Justin for mentioning that, that was on the list of mine, to let the workgroup know.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Any other final thoughts or comments before we open it up for public comment? Okay Michelle, let's open it up for public comment please.

Public Comment

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Okay. Operator, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

If you are listening via your computer speakers, you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. If you are on the phone and would like to make a public comment, please press *1 at this time.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

We do have a public comment from Eric Heflin. Eric, just as a reminder, public comment is limited to 3 minutes, but please go ahead and state your organization.

Eric Heflin – Chief Technology Officer – Healthway, Inc.; Chief Technology Officer – Texas Health Services Authority

Very good, thank you. This is Eric Heflin; I'm associated with the Texas Health Services Authority and Healthway for the eHealth Exchange and HIE Texas. My comment is that it looks like this effort may be redundant with an existing IHE International Standard called Internet User Access or IUA.

One difference though appears to be that this presentation in the MITRE work seems geared around browser-based or human browser authentication whereas the IHE profile is largely geared towards web services type authentication. And this actually dovetails in with the comment I believe from one of the task group members which asked about it being changed from browser to client.

And I think the deeper implication there is that in many cases exchange between entities is not driven by a human actually behind a browser so much as a person working at their EMR or other system and then the EMR or other system such as a health information exchange makes a request on behalf of that human end user. And the deeper implication of that is that means essentially this becomes a system level trust model rather than a human end user based trust model, which has somewhat different requirements.

And my final comment is that many of the other criteria mentioned in the MITRE work also is redundant with existing work. For example, the mention of a certification program for certifying against compatibility and for two-way TLS for mutual authentication; the ATNA IHE profile also has a testing program and IHE International has a newly launched certification program as well, too. So I would advise the workgroup to consider rather than burdening people with yet another certification program, to instead leverage existing industry programs such as those already out there with IHE and others that could be leveraged fully. That concludes my comments and thank you for listening to me.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thanks, Eric. And we have no further comment at this time. So thank you everyone and have a wonderful rest of your day.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you everyone.

Public Comment Received During the Meeting

1. There is an international standard that already profiles OAuth for healthcare use, called IHE IUA (Internet User Authorization). It looks like the MITRE work is largely redundant with the IHE IUA profile. I suggest that the MITRE work be reconciled with the existing standard rather than creating yet another way to do the same thing.
2. References http://wiki.ihe.net/index.php?title=Internet_User_Authorization
http://www.ihe.net/Technical_Frameworks/#IT and
http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_IUA.pdf.
3. Note to operator: Please add these comments to the public record. At the end of the call I intend to make these comments during the public comment period.