



**HIT Standards Committee
Transport and Security Standards Workgroup
Final Transcript
September 22, 2014**

Presentation

Operator

All lines are bridged with the public.

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

Thank you. Good afternoon everyone this is Michelle Consolazio with the Office of the National Coordinator. This is the first meeting of Health IT Standards Committee's Transport and 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. Dixie Baker?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

I'm here.

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

Hi Dixie. 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. 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. 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. Jason Taule? Jeff Brandt? 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. LeRoy Jones? Peter Kaufman?

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

Here.

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

Scott...hi, Peter. Scott Rea?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert

Present.

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

Hi Scott. Sharon Terry? And Steven Lane?

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

Hi, I'm here.

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

Hi, Steven. And from ONC do we have Julie Chua?

Julie 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, I'm here.

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

Hi, Julie. And with that I'll turn it to you Dixie and Lisa.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, I was thinking you were going to start at the beginning of our meeting, Michelle, talking about the rules of the road that ONC has established?

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

Sure, I can kick things off. So, first of all thank you and welcome everyone for joining the first meeting of the Transport and Security Standards Workgroup. Can you go to the next slide? First slide in the deck, one more.

Okay, so, as you all may or may not be aware, we at ONC have restructured the Workgroups of both of our Federal Advisory Committees so we have the Health IT Policy Committee and the Health IT Standards Committee. So, this is a Workgroup that falls under the Health IT Standards Committee and is one of our newly restructured Workgroups. It is actually the first Standards Committee Workgroup to get kicked off.

As you can see here these are our new Workgroups. So, we have a Steering Committee that will help us identify where recommendations from the Policy Committee should be assigned and then underneath the Steering Committee we have a Semantics Standards Workgroup, a Content Standards Workgroup, Transport and Security Standards which is this group, Architecture Services and APIs, and then Implementation, Certification and Testing.

As we have discussed in past Standards Committee meetings the kickoff for these Workgroups will be staggered a bit based upon some of the other work that is happening from the old Workgroups and some of the current work that we are doing related to interoperability. So, for example we have a JASON Task Force that was formed and so once that Task Force concludes then we will kick off the Architecture Services and API Workgroup. Next slide.

So, this is our membership list. Dixie, I don't know if you want to take some time and let each member introduce themselves or if that can be saved for another time, I'll defer to you?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes, I would like to do that, yes.

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

Okay, maybe we can just go down the list, maybe Dixie and Lisa you can kick us off and then we'll go down?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

You might want to go through the rest of the administrative information and then we'll start the real content of the meeting with introductions.

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

Okay, so let's get the slide but we'll come back to it.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes.

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

All right, next slide. So, just a reminder that...and I'm sorry that the red text was supposed to get turned to black. So, now that we have restructured our Workgroups we are looking to make sure that we have active engagement across our Workgroups and a diversity of perspectives.

We're also trying to work a little bit harder to keep our members engaged so we are working towards having two meetings a month for this Workgroup and we hope to have agendas and materials at least 24 hours in advance, it would be great to have it even sooner than that.

And we are asking that members try to be actively engaged and members missing more than five meetings will be asked, within a year, will be asked to be removed from the group. And you can see we are going to be sharing the membership attendance publically so all meetings have a summary and within that summary is the attendance so everyone will see who is attending and who is not. We are hoping that will help us keep up with attendance and make sure that everyone is participating the way that we had hoped they would.

We'll also be reviewing membership on a quarterly basis for active participation and on an annual basis to make sure that we're getting out of the Workgroup everything that we had expected, we have the right perspective on a group and we may need to re-evaluate membership at different points in time based upon the engagement of the group.

In addition to being actively engaged we also hope that members take the time to review materials beforehand so that they can provide the expertise and experience based upon materials that have been sent and, you know, just make sure that people are actually reviewing materials in advance so we aren't walking through things for the first time on the call.

So, again, we also just want to thank all of you we know you all are volunteers and two meetings a month can be quite a bit of your time but we greatly appreciate you agreeing to participate and sharing your experience in this Workgroup and helping us come to recommendations around transport and security standards. And so, next slide. So, Dixie, I'm not sure if you want to walk through the charge or do you want me to?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, yeah that will be fine, that will be fine, thank you, Michelle.

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

Okay.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

I did want Michelle to go through the administrative things with you guys because as those of you who have been on the Workgroup know some of the things have changed, you know, we are very much aware of what a privilege it is to participate on one of the FACA Workgroups and we also know how fortunate we are to have you all really to give us your time, and we want to make sure that there is mutual respect and mutual commitment as we start out.

As Michelle said, the Workgroups were reconstituted for both Policy and Standards Committees and the Privacy and Security Workgroup was sort of reconstituted as the Transport and Security Workgroup. However, its charge is not all that different.

This group will be supporting...security, privacy and data transport and I would also point out to those of you who were on the previous Workgroup known we already were looking at being responsible for transport so that in itself is the biggest change is in the title, name of the Workgroup.

Some of the examples and these aren't necessarily our work plan, but the examples of items that we will be discussing are how to secure data at REST, extending what we've already recommended, the security for application programming interfaces with the JASON Report coming out and a new Workgroup that focuses on infrastructure and APIs. There will be more emphasis through the Standards Committee itself on securing APIs.

I also want to convey to those of you who may not have participated in the Standards Committee meetings themselves that the Standards Committee is...I won't say moving away from Meaningful Use because that's not exactly right, but we certainly are moving beyond just Meaningful Use to a more comprehensive approach to recommending standards for certification of EHR technologies.

So, Jacob Reider, at every meeting he starts out emphasizing that fact that we really should not feel constrained by the Meaningful Use regulation but that we really should be thinking more broadly about what actually should be included in certification of electronic health record technology.

The emphasis is also, you know, primarily, not primarily, but the emphasis has been shifting for the past couple of years to more simple and RESTful approaches to APIs that are not only simpler to implement but simpler to understand, simpler to secure and also that work on those mobile platforms as well as enterprise systems. So, there is more emphasis in RESTful standards and RESTful approaches.

We'll be addressing consent management technology managing individual's consents, permissions, preferences, digital identity which is the topic that we're going to be focusing on today a little later on.

And finally, data provenance methods of recording and conveying the source of data now what that has to do with security is it mostly has to do with data integrity because the integrity or the trustworthiness of data is in many ways related to the provenance of those data where they came from and how much you trust the source of the data. So, that's the charge. Are there any questions? Okay.

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

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Yes?

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

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates
Yeah, hi, Peter.

Peter N. Kaufman, MD – Chief Medical Officer & Vice President Physician IT Services – DrFirst
Hi, I don't have any questions about the charge or what the committee is doing but I do have a question about the meetings. I know we're scheduled for every two weeks, if we're going to be held to missing, you know, to attending 22 meetings a year that's going to be very tight on my schedule and possibly other people's schedules too. I don't know if other people have more time than I do. Are the meetings going to actually be every two weeks and we're going to be held to five meetings a year? Because I won't be able to make that, to missing only five a year.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

The...I'm glad you asked that question Peter, the meetings are scheduled for every two weeks and, as Michelle and Julie will certainly tell you, that really is related to the how difficult it is to get on the ONC FACA schedule because they can't really schedule, double schedule a given time slot and so we wanted to reserve our time slots throughout the year.

We will have meetings when they are necessary and only when they're necessary. So, if we have a meeting scheduled and we don't have any tasking to be working on the meeting will not be held and we'll have an agenda for every single meeting so it will be clear to you what we'll be focusing on and what is expected of you.

The number of meetings to be missed in number, you know, the real criteria for remaining on the Workgroup is really something that comes out of ONC so I'd prefer that Michelle answer that part of it. Michelle?

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

Yeah, I think Dixie...so we've identified five as the number and with the discretion of the Chairs in the standard operating procedures that we also distributed with this meeting there are more detail about that in there. We understand that there might be extenuating circumstances that come up and we know that our FACAs are very busy.

This is really just to eliminate people that never attend meetings and are just listed on the roster and may not be actively participating. You know if you're missing six meetings we can evaluate it, but we did pick five as the number and we can re-evaluate if that's necessary.

And as Dixie mentioned the meetings will ebb and flow for those who have been part of the FACA process in the past depending upon when the Workgroups are charged with items sometimes they are meeting maybe even more than twice a month and sometimes we may not need a meeting at all. So, as Dixie said we'll have to adjust accordingly but, you know, hopefully you'll be able to make as many as you can.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

And I would like to stress what Michelle said about extenuating circumstances. If you're not going to make a meeting by all means let us know that in advance. We really appreciate that. It really helps us understand what is going on and whether to wait for you etcetera, so, you know, we're all human; we all have other demands on our time. So, if you do have extenuating circumstances please do let us know.

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

So, Dixie this is Lisa, may I add something?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes.

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

I think, you know, the most important part for us is active participation. We have some challenging tasks on our agenda for the rest of this year and, you know, if...one thing that is helpful is if you're going to miss a meeting but you've reviewed the materials and you have some input for us if you could send that along as well. I think, you know, everyone that is on this group is, you know, very experienced and has a perspective that, you know, it is particularly important for us. So, I think that's important to stress too.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes, yeah, thank you. Okay, with that Michelle why don't we go back to the slide that has our members and I'd like for everybody to introduce themselves. We've sort of gotten into the conversation I probably should have gone ahead and introduced everyone at the outset.

I'm Dixie Baker and I Chair this committee. I've chaired the Security Workgroup since it was formed and I have a background in security forever and I'm a consultant, I'm a Partner with Martin, Blanck and Associates which is a healthcare consulting company. I live in Redondo Beach, California. So, Lisa Gallagher is my Co-Chair, would you like to introduce yourself please?

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

Sure, thank you, Dixie. I'm Lisa Gallagher I'm Vice President of Technology Solutions at HIMSS. I've been a member of the...well, I was a member of the Privacy and Security Workgroup for a couple of years and then became a full member of the Standards Committee and I guess it's probably about six or eight months, maybe longer, when I started to serve as Co-Chair of this group.

I have a background in security as well, I'm an engineer by background and I was a security consultant before coming to HIMSS eight years ago. Dixie and I have known each other for a long time and we're privileged and happy to be continuing to work on these challenges on behalf of the healthcare sector. Dixie?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Okay, thank you. Now let's just go down the list. I think the next one who is here is Brian Freedman?

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

Yes, hi, my name is Brian Freedman I work with an organization called Security Risk Solutions. I'm here in Charleston, South Carolina. We do a lot of work around with Health IT privacy and security and we actually have some other members of the team that actually do some work with ONC as well already. In the past I was...more recently I was chief information officer of one of the larger primary care practices here in South Carolina so there was a lot of change and growth that we saw, especially with a lot of the Meaningful Use and privacy and security and all the different rules that we had to kind of deal with on a day-to-day basis.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thank you, we're happy to have you as a new member to this group. John Hummel?

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

Hi everybody I was a member of the four HITSP committees including the Data Security and Transport when they formed them with John a couple of years ago and prior to that I was a Co-Founder of CCHIT which I'm unfortunately seeing them getting out of the certification business now. I was CIO for Sutter Health it's one of the larger integrated delivery systems.

Then I was federally court appointed to the California Prison Receivership where they were killing one inmate every five days by medical mistakes and data security took on a whole new meaning for that.

Then I went onto become the Chief Technology Officer for Pro and Dell Computers for Healthcare and now I'm up here at beautiful Lake Tahoe, which is a little smoky today, at a wonderful little CAH hospital where we're putting in a whole bunch of software and most of it is data driven, data security driven and I'm about four weeks from completing my Master's Degree in Data Security and Data Assurance so this is very important to me and I feel very privileged to be on this committee again and I'm looking forward to working with you guys.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Well, we're happy to have you, John, thank you.

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

Dixie, I think LeRoy Jones was able to join if we want to go back to him.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Oh, okay, LeRoy, Lee are you there?

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

I am, are you able to hear me?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes, hi.

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

Hello. My name is Lee Jones I'm the CEO of GSI Health we are a software as a service vendor in the care coordination space so we deal with, you know, these privacy and security issues all the time in our role as curators for data for our customers as well delivering it through software and interfacing with other systems, etcetera. And I've also, you know, done work in the past with HITSP and with a number of the ONC initiatives in various capacities including these privacy and security topics so happy to be asked to be a part.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, we're happy to have you Lee. Okay, Steven?

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

Hello, I'm Steven Lane I'm a practicing family physician and clinical informaticist at Sutter Health in Northern California. I used to work with John when he was here. I'm returning to the Workgroup space. I worked with CCHIT for a number of years Co-Chaired a number of their committees, also worked with the California Office of Health Information Integrity on their Privacy Committee for a while. I do work at our enterprise as the physician lead on issues of privacy, security and on health information exchange. We've done a lot of work with the Epic platform here and are moving in the direction of an enterprise HIE so have a lot of interest and a bit of experience and looking forward to working with the group.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Good, we're happy to have you Steven, thank you. Peter?

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

Hi, I'm also a practicing physician, a gastroenterologist; I practice part-time in the Bethesda, Maryland office of my 55 gastroenterology group. I've worked for DrFirst as the Chief Medical Officer for the past, just shy of 15 years. I probably know less about security and transport than anybody else on this committee although our founder invented work for private networks, so I can try to draw from him.

But, I was on the Privacy and Security Workgroup and learned much more from being on that group and I have been adding to it and I hope to continue learning and participating in this committee. I was on CCHIT's ePrescribing Committee and worked on the CCRNA SDM and I continue to be very active in NCPDP with ePrescribing standards.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thank you and we're happy to have you. Okay, Aaron?

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

Yes, hey, good morning or I guess good afternoon, potentially wherever people are right now. My name is Aaron Miri I'm the Chief Technology Officer for Children's Medical Center here in Dallas, we're the fifth largest pediatric hospital system in the country. We have one of the busiest EDs in the country however. We've been instrumental in working with the State of Texas on a...in their first...as the first health system awarded the Texas Privacy and Security Certification.

In addition, we worked with HITRUST extensively to become HITRUST CSF certified. We have also worked with the ONC on the Ignite Project enabling one of the first pediatric PHRs in the country in combination with HealthVault and Verizon, and Epic.

So, we constantly strive to look at everything we can do as a forward facing pediatric organization in addition to ensuring that all of the privacy and security principles are intertwined with everything that we do. So, from a degree of what we're able to bring to the table and what I'm able to contribute I'm absolutely excited and delighted to be part of this group.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thanks, we're happy to have you. And Scott?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert

G-Day my name is Scott Rea, last name is pronounced Ray, looks like R-E-A but it is R-A-Y as in ray of sunshine. I think I'm at a disadvantage because it's going to be fairly easy I think in this group to pick out my voice, it might take me a while to learn other's voices. Originally from Australia I've been in the US for 15 years. I'm out in Utah a place called Lake Shore.

I'm employed by DigiCert. DigiCert is a commercial certification authority they do identity and security for websites and authentication as well for websites and documents, and code signing, etcetera. I am VP of Government and Education Relations at DigiCert so I have a role in relationship management in government and research space, but I also have a technical role at DigiCert I'm the Senior PKI Architect. PKI has been my specialty. I've been working in that field for longer than I care to recount.

I also have actually been, as an independent consultant, supporting the Department of Health and Human Services for over a dozen years, their own internal PKIs and I've been participating with the federal PKI and the federal bridge, and controls and standards and policies around PKI-based implementation very familiar with those from a federal government perspective.

More recently I've been working with DirectTrust. If some of you are aware of the DirectTrust initiative it is in setting up policy and standards for the implementation and operation of Direct. DirectTrust actually has a grant from ONC to set up a national trust community and I'm actually a board member on the DirectTrust initiative as well.

I have been working also with some of the ONC Workgroups for the federal health architecture and continue to participate there. Very much looking forward to participating in the conversations and perhaps providing some good input where I can.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Great, great it's great to have you. Obviously you'll be very interested in today's discussion. And Scott's comment about his accent reminds me that I wanted to reiterate what Michelle says is when you have comments, and this will take some getting used to I'm sure, but it really is important that...this is a public meeting we have others listening in and besides the fact that we don't yet know each other's voices, so when you make a comment please start out by stating who you are. So, with that we...today's...one of the...

Jeff Brandt – mHealth & Security Consultant

Hey, Dixie?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes.

Jeff Brandt – mHealth & Security Consultant

This is Jeff Brandt I'm on the call.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Oh, hi, Jeff would you like to introduce yourself?

Jeff Brandt – mHealth & Security Consultant

Yeah, I've been having all kinds of problems with Adobe connect so I finally got on the phone call. So, yeah, I'll introduce myself. I'm Jeff Brandt. I'm a consultant with...and I've got a long history of security from back in the 90s and before that I was a telecom engineer so I have a lot of experience in moving data to the phone system and secure.

I've got a background in computer science and medical informatics from OHS Medical School and I've been a participant in many of these discussions with HL7 and on HIMSS, and co-wrote some books...is one of them...I worked with in the past on security for mobile devices which is I work a lot in the mobile sector. So, glad to be here.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Okay, good, I'm glad you were able to dial in. Okay, is there anybody else that I may have missed that might have joined us a little late? Okay, for the past, at least year, the Security Workgroup has been following the NSTIC, the National, let me see, Trust, what is it, NSTIC.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert
National Strategy for Trusted Identities in Cyberspace.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

That is it, I couldn't remember what the "s" was because I kept going security and I knew that wasn't right. Yeah, the National Strategy for Trusted Identities in Cyberspace, the NSTIC and we've had a public hearing on NSTIC. Whenever we do recommendations for certification criteria we keep NSTIC in mind and we've been...and it certainly is a primary initiative that we're watching.

So, today we're going to hear from one of the NSTIC pilots, the one that is in Georgia and our speaker is John Wandelt who is the Executive Director of the National Identity Exchange Federation at Georgia Tech Research Institute and he will tell us about the Trustmark Pilot there. Lisa has known John and known of the Trustmark initiative for some time. So, Lisa, would you like to add anything in that introduction?

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

Well, just by way of background we do talk quite a bit on the Standards Committee and on this Workgroup about the challenge of trust between HIEs or trust between trust frameworks and, you know, when I learned about this pilot I thought it would be interesting for us to hear about how they've constructed the Trustmarks and how trust can be componentized and could be digitally exchanged and I think the concepts that they have here are interesting for us to consider.

So, I want to thank John in advance for being here and looking forward to a good discussion after he does his presentation. So, thank you.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, thank you, Lisa, thank you for connecting us and Julie as well. Okay, so with that can we bring up John's slides about the scaling interoperable trust?

And by the way for those of you who may not be used to this meeting interface that we're using all of the materials that we're using in today's meeting can be downloaded through the download window on the left side of your screen, just click download files and you're able to download the PDFs to your desktop. So, John, thank you very much for joining us today.

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Well, thank you so much for giving me the opportunity to share about our pilot project with the group. Can everyone hear my voice?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes.

M

Yes.

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Great, okay. So, I'm with the Georgia Tech Research Institute which is the applied research arm of Georgia Tech. I also want to thank NIST for sponsoring this work. This presentation has some animations built throughout the deck so from time-to-time you're going to hear me say, click, click and whoever is remote controlling this if they would just give it one click I can talk as we build out some of the animations and we go forward.

I'll spend a little bit of time up front kind of giving you the motivation or the why we're doing what we're doing and I must say that it is an impressive group of individuals hearing your introductions on the phone today so a lot of you will probably, through your various experiences and history, realize some of these same challenges that led us to this project.

So, let's start with the first slide here and as we all know we're more and more connected today, we're sharing with partners in different use cases than we originally anticipated maybe 5-10 years ago. And when we think about trusted information sharing even in the simplest sense where there is a direct trust relationship between let's say a producer or consumer either for sharing information or some kind of trusted transaction there is typically an MOU, there is an agreement and that agreement includes, you know, many technical details in terms of protocols, profiles, certain business aspects or legal aspects and so forth, but there is an agreement. So, click. Next slide.

And so as we start to think about scaling out this agreement there is typically more details, there needs to be more rigor in those details in terms of documentation. We no longer have direct trust as the numbers of producers and consumers increase. We don't have those direct trust relationships. We rely on third-party types of trust models and one of the challenges of course is we move at the speed of agreement in lots of different dimensions. Next slide.

So, as policy makers and architects the challenge is finding that balance where we can make sure we maintain the proper security interoperability, privacy, trust as we begin to scale out to these new relationships and to do this in a way at a low cost and hopefully in a way that we don't really penalize our early adopters in the ecosystem. So, next slide.

Now the challenge with agreement is agreement is hard to scale and we've probably all lived this in various different committee meetings and, you know, NSTIC is a large group with large diverse stakeholders and as the number of participants and communities of interests, and use cases increase what we find is we need to get more and more agreement but in reality what we end up getting is very often less agreement and we tend to abstract that agreement to higher levels in terms of maybe just high level principles which very rarely can get us the intended outcome and the value proposition. So, next slide.

So, identity is fundamental to solving this problem. Trust is fundamental to solving this problem and one of the groups we work with is the National Association of Chief Information Sharing Officers and every year they do a survey of the CIOs and identity and identity management always come in the top ten sometimes in the top five and there are a number of barriers that they continually site and I think you see them in health and we've seen them in our communities as well, challenges of a decentralized environment, the cost of doing this, the complexity and finding the right kinds of governing structures that can be employed to get the kind of agreement we need, broad scale agreement on many dimensions. So, next slide.

So, this is where NSTIC, National Strategy for Trusted Identities in Cyberspace, really plays a role here, it's a White House Initiative, public/private partnership with the goal of elevating trust in on-line transactions, on-line information sharing and so forth, very broad scale. The intent is to cross multiple communities of interest even go beyond a national perspective to an international perspective.

The identity ecosystem steering group is the private part which has representation of multiple communities of interests, multiple working groups that participate. There are a series of pilot projects that have been funded, ours is one of those, that inform the various different working groups there with real world concrete experience in feeding that in and our Trustmark Pilot Project has been getting quite a bit of interest across all of the committees and across all of the pilots in NSTIC to date. So, next slide.

So, just to step back for a second to look at how identity frameworks and some of you have lived through this I'm sure with your experience how they've evolved. You know we used to have our identities locked in what I would call application silos, it was an afterthought. We had user name, password, we had both on security, we tend to move from that because we have more applications, we wanted to build in efficiencies, we've moved to an enterprise perspective where many applications fall under the span of control of some kind of organizational structure, organizational boundaries and we've employed VPNs and virtual directories to try to solve that problem but as we began to span out to partners in other organizations and different use cases we've moved through this federation model and technologies like PKI that was mentioned and SAML and OpenID Connect helped facilitate that third-party trust and the mechanisms for employing federated type of solutions out there, but federated solutions tend to be, in practice, focused on a particular community of interest.

And where we need to be going, based on the state of need, is really to a more ecosystem approach, cross sector or marketplace and so what kinds of solutions and tools do we have to facilitate that, basically unlocking our trust identities in the work that we do to participate in one community of interest and to leverage that at a lower cost into other use cases or other communities of interest. So, next slide.

So, in the beginning our identities are locked in application specific silos. Next slide. Along comes federated identity separating the identity provider from the application provider. We decouple that identity providers, as many of you know, do the identity proofing, the vetting of the user, they credential the user, they authenticate the user or the applications of the relying party. They own the data or the function of the service. They know the rules. They are responsible for auditing access and applying those rules, but now that these functions are no longer under the same organizational boundary, we separate those roles across organizations the question really becomes, well how do we maintain that trust, the liability concerns, the security, the interoperability and so forth? Next slide.

So, what we've seen across the landscape is a number of formal trust frameworks that have emerged and a lot of these frameworks don't call themselves trust frameworks, they may be federated environments, they may be information sharing environments or so forth and here is just a sampling of those. The goal of these trust frameworks are to establish a common set of operational policies and procedures, basically a baseline agreement, that all that subscribe to or all that on-board or join it reduces the cost, the friction and increases the velocity of transactions among the membership there. So, next slide.

So, where this leads us to...okay, so there is a little bit of animation here that doesn't seem to be playing out in this slide, but I'll...oops, back one, okay. So, I'll just describe this here. So, really today there are many different trust frameworks that have emerged they are all slightly different, they all require many dimensions of agreement and they tend to be what I would say as monolithic and opaque. You are either a member of that club or you're not a member of that club and it's very hard to discern what the differences are between two trust frameworks without really being an engineer and doing quite a bit of analysis to compare the delta between those two trust frameworks. So, next slide.

So, the question becomes if you are a member of either as an identity provider or an attribute provider or relying party of one of these information sharing environments these federations or these trust frameworks how does a user in your trust framework get access to a relying party in another one and that basically is the \$25,000 question that we've all been thinking about that, but there are lots of ways you could imagine that could happen, you know, you can join multiple trust frameworks or your identity provider could join multiple trust frameworks or relying party, but none of those scale very well and they're expensive. So, next slide.

So, I've been involved over the last two or three years in many discussions about the notion of inter-federation and what is inter-federation and what does it take to inter-federate and so forth. And the group of engineers I work with here and many others are beginning to believe that inter-federation is very difficult to do and for some of the reasons that you can see on the slide right here.

No two federations or trust frameworks are identical. So mapping between them becomes difficult especially when you don't have that transparency. They tend to be moving targets. We're really in the early days here so things are evolving and they're evolving quickly so any time you try to map or build a gateway by the time you're done they've changed right there.

Transitive trust tends to be what I would call diluted trust. If federation A has an inter-federation agreement with B and B has one with C does that mean A and C should try to, so it doesn't really scale as a number of federations scale.

And then probably the nail in on the coffin on this, and we've lived this firsthand, is that contractual obligations between the members of the federation or a trust framework into the trust framework do not really work across the inter-federation boundaries there are lots of difficulties with that. So, next slide.

So, where we've come full circle where identities used to be locked to application silos and how they are really locked and what would call trust framework or federated identity silos. Now the silos are certainly bigger and they certainly solve some problems but as we look to cross sector trust and being able to handle in an agile way change even within membership of a trust framework we need to think about this slightly different. So, next slide.

So, wanted to give you the perspectives of a community that we supported for the last two decades law enforcement, public safety this is the community that we're initially piloting our NSTIC pilot in and you'll see a lot of common things across large communities, there are over 1 million law enforcement officers, they are highly decentralized, there are tens of thousands of agencies some are haves and some are have nots, some have big infrastructure, some have hardly any resources at all and are very small. They have a legitimate need to talk with each other. They must obey the rules and regulations that are set forth for sharing different kinds of information.

They do need to talk with other communities of interest health, they need to talk to mental health and substance abuse counseling, and critical infrastructure protection and so forth. So, there is a lot of cross COI need there. They are very heterogeneous. Next slide.

So, the question that has been asked and all along was, well what if I could get a strong credential from my home agency that would work with my applications and then would also work with my partners across other community's interest, across state, local, regional and federal boundaries. Next slide.

So, this was the question that was asked after 9-1-1 one of findings was that the right people weren't getting access to the right information. We had all the information. We couldn't piece it together to solve the problems that we needed to solve and so another Federal Advisory Committee, called the Global Information Sharing Initiative, started under Janet Reno that reported to the Attorney General under the Department of Justice, the Security Working Group of that FACA, I sat on that group, and through a series of discussions and meetings much like this and lots of work done a set of products called GFIPM, Global Federate Identity and Privilege Management, evolved. Next slide.

So, now one of the things is these standards and these profiles of SAML and best practices called GFIPM evolved one of the challenges was that a lot of little GFIPM federations began to emerge throughout the country that did not trust or interoperate with each other. In addition, there were other federations or information sharing environments that also law enforcement needed to talk to.

So, in 2008 key stakeholders in the law enforcement...safety space got together and we established the National Identity Exchange Federation with the goal of sharing trusted identity and attribute information about users and end-points among the membership effectively trying to knock down the silos that were beginning to build up even with this federated identity technology and even with trust frameworks that were beginning to emerge. So, next slide.

At that same time the macro environment in this space was getting noisy and what I mean by that there were a number of programs, initiatives coming out of the federal government that tended to overlap addressing different parts and when you have a lot of those kinds of, what appeared to be competing programs even though they are slightly different but they're overlapping, the state and locals that typically don't have a lot of funding they stop, they don't do anything. They look there and they said, well, let's let the feds get their act together or let's let the solution, you know, evolve and when we get to a certain point then we'll adopt it, so you get that deadly embrace.

So NIEF began to get involved in all of the major initiatives in the space including FICAM, Federal Identity and Credential and Access Management, coming out of the federal government. For example, we submitted an application to be a FICAM LoA 2 and LoA 3, a trust framework provider we expect to have that in place in the next month or less and several other initiatives NSTIC being one of those we'll talk a little bit more about. So, next slide.

So, we began to ask ourselves here with all these new initiatives out there and with a set of practices and standards we put out that began to get uptake but still drifted and didn't have the fundamental basis of trust in place. Where do we go? How do we start to tie these silos together again without punishing early adopters and thrashing a particular...a community that can grow fairly large and is going to evolve over time? Next slide.

So, this is what led us to put a team together and put in the application for our pilot, which those of you who have been through the process know it's an extremely competitive process with a lot of rigor and review, and so we put the pilot in for scaling interoperable trust in a Trustmark marketplace, this was where the idea of the Trustmark came at, I'll explain more about that. Our partners include NASCIO, include faculty on Georgia Tech and GTRI, and also the members of the National Identity Exchange Federation. So, next slide.

So, fundamentally in thinking about the problem our approach is what I would call componentization. What if frameworks, trust frameworks, federations were more modular they used some standard components, okay, this would give us greater transparency, greater ease of comparing frameworks, potential for reuse. So, this is the same fundamental approach we applied to the National Information Exchange Model, NIEM, I'm not sure if there are those of you who have heard about that, I've been involved in the NIEM program as, I'd say, running the engineering team since inception even before it was NIEM when it was GJXDM, the Global Justice XML Data Model, it actually came out of the same FACA that GFIPM did and leading to this work as well.

And so, if we had components and we could reuse those components and standardize those components and do that in a way where components could be extended and they could be constrained we could get that agreement. So, next slide.

So, we call these components for the purpose of our pilot project here Trustmarks. Now you could view Trustmarks think of them as almost mini-certifications, mini-certifications that are intended to be reused and repurposed for different business context depending on how you bundle them together. So next slide.

So, Trustmarks can be defined for technical aspects, trust, privacy, security, different business aspects even handle the legal aspects. Since they are machine readable they can be digitally signed in order to give them certain security properties, think of them almost like digital certificates X.509 certificates in a PKI realm. They can be automatically processed. They can be totally transparent to an end-user or you can bundle a group together and associate it with branding some kind of an icon that means something if you want to convey trust and meaning all the way down to the end-user. So, next slide.

So, let's see how these play out in what we would call a Trustmark-based identity ecosystem. So, existing trust frameworks or federations would define what we call a TIP, a Trust Interoperability Profile, it's a bundle of Trustmarks that represent their existing agreement. Members, next slide, sorry, so members of the existing trust frameworks or federations would acquire these Trustmarks based on that trust interoperability bundle defined by their community of interest, they would require those. They would get those from what we call in our framework Trustmark providers.

The initial Trustmark providers in the ecosystem will likely be those that are already the federation managers, those that are already the trust framework providers and so forth. But over time multiple Trustmark providers can exist for the same Trustmark whether it's a Trustmark issued for some privacy aspect or a Trustmark issued for some interoperability aspect with conformance to a certain profile or so forth. Next slide.

So, these Trustmarks, these standardized reusable components can then be published, stored into registries that can then be searched and discovered by members not only within a single trust framework or community of interest but across communities of interest and across frameworks.

So, the goal of making these components transparent is that you would get convergence and reuse of various aspects over time. Now that doesn't mean that every trust framework, every community of interest uses every mini-certification that there will be some that are used that are meaningful within a law enforcement context, a set of attributes for example that identify a law enforcement officer which would be different than a set of attributes that might identify a nurse or a doctor, or so forth, but some of the fundamental underlying technologies and agreements in place can be reused across multiple context. So, the intent of the Trustmark is to unlock work that you've done as an actor for multiple contexts. So, next slide.

So, our NSTIC pilot work falls into six major categories here concept maturation for the Trustmark concept, the development of technical normative specifications for a Trustmark framework, actually to build some of these what we call Trustmark definitions, build the components themselves, build some sample tools which we're going to publish in the marketplace in terms of open source, to pilot this in the National Identity Exchange Federation among state, local, federal law enforcement agencies and then to expand that pilot beyond law enforcement initially they'll expand on the fringes, we have some pilots identified with mental health and substance abuse counselors and so forth.

The first four of those goals right there we've made very significant progress I'll point you to a website you can get into the detail of those so we've completed a lot of that. Our initial operating capability of deploying this technology in the law enforcement sector is going to be the end of this month. So, we've made a lot of progress and then a lot of our second year in the pilot will be expanding out to other use cases and propagating this out and lessons learned and feeding it back in. So, next slide.

So, one of the things that we had to do, this is a new way of thinking about the problem, and one of the things we had to do was to define a formalized model of who are the actors in a Trustmark federation or framework, what are the roles and responsibilities and so forth so I'll just walk through this briefly.

In this model there is a stakeholder community it is represented by what we call a Trustmark defining organization that kind of maps to maybe your existing standards, SDOs, today, it could map to a committee like this. In our world it's going to map back to the FACA that we support for justice of public safety.

So, there is a group and that group is responsible for defining a set of concrete requirements and assessment criteria and they capture those in a formal what we call Trustmark definition and we have a standard for capturing that in a standard way and there is a methodology of walking through existing requirements, harvesting them out and articulating them in a well-defined standard, machine readable way.

Those Trustmark definitions since they are represented in a consistent way of not only a set of requirements but also assessing those requirements they are used by Trustmark providers which are effectively your assessors and they walk through those on behalf as a Trustmark recipient, those Trustmarks are then issued or mini-certifications to the Trustmark recipient by an assessor or a Trustmark provider following that assessment process defined by a group. So, defined by this group on the phone they would define for a particular aspect and that would be captured and then assessors in the marketplace could then issue those assessments in a consistent way to recipients.

And then relying parties, Trustmark relying parties, would rely on those mini-assessments, bundle them together for particular business context and that would provide the context of a trust framework or a federation or so forth. So, next slide.

So, one of the questions, you know, that you ask is, well where do these requirements for these components, you know, come from?

And it's not the goal of this framework to reinvent any new set of requirements, it's really to capture them and to articulate them with well-defined assessment process in these mini-certifications to unlock work that you've done, an assessment you might have already done, an audit you might have already done in a way that can be then leveraged in another context in a machine readable format that can then be searched and picked up.

So, as part of our project and I'll show you in a couple of slides here some of the ones we've harvested, but there is no shortage of harvesting them out. You look at your common...many of the trust frameworks out there have lots of requirements that they've identified, we've gone through as part our pilot project many of these trust frameworks and harmonized components out of those trust frameworks. You've got things like the Cloud Security Alliance which has a matrix of 138 requirements in there perfect for harvesting out standards for or components for security, privacy, trust, interoperability, accountability and so forth. So, next slide.

So, we talked about capturing these requirements in a well-defined format. There is a specification, one of the specifications that are being published under our work here eventually it will go into an SDO, but it will be published to our website probably in the next month, we're using it internally, is what we call the Trustmark Component Definition Specification, it has a schema for capturing the various aspects of the requirements in XML with translations for human readable HTML as well. So, next slide.

I'm just going to hit...there are several different components when you...several different parts of capturing the requirements for one of these Trustmarks, the two that I'll just highlight, one is conformance criteria and this slide was supposed to build out, it's kind of covered right now, but I wanted to show you an example for...this example here is FICAM LoA 2 authentication process that would be a component.

If you satisfied the conformance criteria for that you would get a mini-certification for that part and whether you use that to be an identity provider to FICAM or you use that same normative conformance for another purpose whether it's for health or in the community for law enforcement the conformance criteria is consistent, it's well documented and the other part I'd like to highlight there is an assessment process.

So, one of the challenges that we have in standards is there is always lots of optionality in standards and my experience very often is there is... and we have vendors that will claim or products in trying to assess whether a product actually meets a conformance criteria or is the characteristics of a particular spec and it's hard to assess that very often without doing a lot of testing.

Built into the Trustmark Component Definition they have an assessment process that says, any assessor that issues a Trustmark for this particular component must do these things and it clearly lays out those things, they must answer these questions, every question is a yes or no answer and it may ask you to upload some evidence and I'll show a little bit about that in a couple of slides coming up here as well. So, next slide.

So, as part, like I said, of our particular pilot project for the community that we're going to demonstrate this in we've developed on our website, there are 60 published here, there will be about eighty of these, Trustmark components or mini-certifications that's not reinventing things, not inventing new requirements but basically harvesting those requirements and harmonizing those out of things like FICAM, Kantara frameworks, the NIEM framework and common framework and so forth to take a look at common elements, common conformance criteria and assess and process, and then factoring those out at the right granularity.

And the right granularity really in the context of this approach is granularity that gets for reuse, it is not...don't make it granular just to make it granular you make it granular because it can then be reused across multiple business context. So, you can see some examples here, for example registration and issuance requirements for a Level of Assurance 2 or registration issuance requirements for Level of Assurance 3 might be some examples of components that you could get a mini-certification or a Trustmark for. Next slide.

Just continuation of this, one thing I'll note here, we also did some of the FIPS security requirements, audit and accountability is an example, personnel security and so forth. If you hit our website you'll see that these are published in both the normative XML, those requirements, and also through a translation a human readable HTML version as well. So, next slide.

So, these requirements, these mini-certifications can then be assembled in bundles for particular business context so much like again in the NIEM world instead of having lots of different independent information exchange that all reference a person or a doctor, or so forth differently, reuse that same component so that we gain greater understandability of that but use it in different context but it means the same thing it's represented the same way.

These bundles that you can put together...here is a sample that we put this slide and the next slide together for the identity ecosystem steering group to convey that for example if the business context was SAML requirements for identity providers, IDPOs, Identity Provider Organizations, it would look something like this or it could look something like this and you can look at the various different components. There would be some token and credential management requirements, there would be some assertion requirements, there would be some ongoing verification requirements.

And for each of those requirements you could say that there "must exist" and if it "must exist" who must you get it for? It's much like in the PKI realm where you have digital certificates but not necessarily everyone trusts the same certificate authority. So, here you can specify.

So, in this for example, right here, registration issuance requirements, you must have that to conform to identity ecosystem, SAML requirements and you must get that from an approved trust framework provider. So, that's an example of how these bundles work.

So, a lot of flexibility, a lot of options for extending by using the exact same component in a way that you would get them from different Trustmark providers because your community of interest has different trust anchors, different optionality in terms of what you must have or what you should have. Some of these components may be totally optional in your profile. So, the next slide.

Next slide is fundamentally a continuation of that just playing out this example. So, we put these two slide's together to illustrate with components that we had built what would a, like I said, a trust interoperability profile look like for the identity ecosystem for SAML identity providers. So, next slide.

Now one of the advantages you get with formalizing the way you capture these requirements, what we call the Trustmark Component Definitions, capturing those requirements is that you can automate and you can speak to them. So, one of the things, regardless of what you do at scale there is going to be...you're going to have to create an ecosystem of assessors and assessors that doesn't prevent groups from self-assessing but typically when we want higher Levels of Assurance we're going to rely on third-party assessors and we would like those assessors to get up-to-speed quickly, we'd like those assessors to assess in as a consistent way as possible.

So, we've built an open source assessment tool, it's not quite an open source yet but it will be, but we're using it for our pilot and we'll make it available through the IDSG, such that any of these components that you defined in this manner will be ingested, can be ingested into this tool. So, you say, here's our profile for this health use case, here's our profile for this law enforcement use case it's a set of Trustmark definitions, you identify those. The tool will ingest those and since the machine readable definitions, the specs themselves are machine readable and understandable, it will take that in there and facilitate the assessor through each of the questions that he needs to conduct the assessment against and it will tell the assessor when they need to collect a piece of evidence that's required by the author of that definition or the author of that. So, that's just something that is kind of an added bonus by providing that consistency and so forth. So, next slide.

And so here is just a quick screenshot like I said each assessment step for one of these is fundamentally a yes or no answer and it asks the assessor to upload certain evidence. From the assessor communities that we've talked to we have several discussions ongoing there, they are interested in this because it helps to get that community and the base of people that are already doing assessments up-to-speed quickly and as that evidence is collected it will also say things like the retention of that evidence and because we had a spec it's not all dependent on this particular tool we envision others building tools of their own but we want to seed the community with something that's open source, that's easy to use as part of our pilot as well. So, next slide.

So, really just trying to wrap it up here so that there is enough time for questions, we have a website out there for those of you who haven't seen it here is the URL. We tried to publish most of what we're doing. It may run 30-40 days behind because we have some internal vetting before we publish there. If you went over to the right "what's new" this is an old screen shot but under the "what's new" and you clicked on that you'd see a number of these Trustmark definitions that I took the screen shot for and as you open those you can walk through and get an idea of, you know, what's under the covers in some of these definitions concretely. So, with that said I think we'll open it up to questions or if there is another step here we can do that as well.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thank you, thank you very much for a very good, well thought out, very well presented presentation about the work that you're doing. Now I have a question, so just to be clear the Trustmarks are assigned to organizations not to individuals and the individuals then somehow convey the Trustmark is that right?

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

That's right, so Trustmarks are defined and then bound typically to an endpoint and there is a lot more beef and meat behind the framework itself it's not shown here but you're exactly right.

So, an identity provider, if you're an identity provider today, let me give you an example, in our federation NIEF there is an on-boarding process and identity providers that want to on-board there is some interoperability testing, there is a lot of documentation, there are some audits that are done and after they meet that then they are a member of the club, you know, they're a member of the trust framework, the federation, same thing with relying parties that come in, and so everyone knows as a member of that federation what that means and so that works well.

The problem that we ran into...and so, yes, they get assigned their Trustmarks and they'd be able to look at, you know, those Trustmarks and make decisions. The problem is, as you start to grow out your federation and there are lots of different kinds of actors in your federation they're going to trust and interoperate with each other not exactly the same but in different ways and you start to define those different ways, you have to metadata tag those somehow so they can do that and establish that trust. You could...

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yes...

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Yeah, sorry, go ahead?

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, well that where I see is the principle challenge is that organizations and ecosystems don't trust each other, for example most of this presentation is about FICAM, the federal government and, you know, the healthcare industry doesn't necessarily trust the federal government. I mean, we found this, this is not just my observation, we found this through research into FICAM and how to really share identities, you know, between the federal government and private industry, and the federal government wouldn't necessarily accept a credential that was issued by a doctor for example and the doctor is very hesitant to...and that's what they expressed in our public hearing that they don't want to accept a credential that's necessarily issued by a government agency.

So, getting those you know...this presentation is very government oriented so I can see how it would work there, it's more difficult for me to see how it would translate into our industry that for a number of reasons don't trust each other.

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Yeah, let me address that for a second, because it's actually, in my opinion, almost the opposite. A lot of times the trust doesn't exist because of lack of understandability, lack of transparency, right, and so with the Trustmarks that you assign to various organizations or, you know, actors in the ecosystem, let's say it that way, the third-party mini-certifications do not guarantee that everyone has to talk to everybody, but I may know nothing about, you know, another federation or another identity provider out there, but if I can look at it, what they've published, and understand that they've got this assessment from maybe one from the federal government, maybe another one from a Deloitte or some other kind of auditor, maybe another one from a particular community of interest or trusted third-party, I then make the decision is that sufficient for me whether I'm a state, local, private sector entity and whether I will engage with that.

It's much like how PKI works today with certificate authorities issuing digital certificates through a trusted third-party that issues the certificate under a well known policy and due diligence and we decide whether we want to trust that for us as health connections or so forth.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Yeah, that works in the federal government, but let me...let others make their comments and questions.

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

Sure, this is Aaron Miri and again I'm the CTO at Children's Medical Center so let me talk about this from a provider perspective. Number one, let me commend you on an exceptional job, I'm actually surfing your website right now reading various aspects and it's easy to understand so this is something I can turn around and show other folks that maybe they are not in depth in the security realm but they'd be able to get it quickly, so kudos to you and your team on this.

From a provider perspective I think it's important to note that trust is established when trust is earned and I say that meaning that let's look at how we credential medical providers, obviously they go through an extensive background check, there are extensive, you know, polling of previous locations, validating their medical licensure, board certification all those kinds of things before they're granted the ability to practice medicine in a hospital.

And much like the same instance of how we trust one another with organizations we do our due diligence, you know, with whom we trust in the medical community and obviously somebody that we're closely affiliated with maybe a sister, you know, pediatric hospital or a hospital in the Metroplex of Dallas/Fort Worth, you know, would be a lot easier to trust than say somebody in Alaska, no offense to Alaska, I'm just, you know, stating the farthest location from here in Dallas, but to the degree of it having a framework, having something is better than nothing.

And I think the key in order to capture the healthcare audience in general is going to need to provide a WIIFM, What's In It For Me, aspect beyond just a framework whether it's some EHR cover from the OCR, whether it's formal endorsement from the HHS saying, yes, this framework exactly meets all the HIPAA requirements and therefore if, you know, gosh forbid you do have a breach of some sort you're not negligent, you try to do everything you possibly could to do best practice, things just happen. I think that's the missing aspect that I think any framework, this framework or any framework is missing is that WIIFM.

And I think it's upon us, as the healthcare industry, to take these kinds of notions and say, look there has got to be some sort of element of understanding of going, okay, you're doing your best hospital A, B, C, you're trying your best things do happen, you do have nations, states and rogue actors doing things or potentially an employee goes rogue and no matter how good a framework you do, no matter if you put this in and you have Trustmarks established things could still happen. So that WIIFM is what's needed I think at the end of the day. I just wanted to throw that on the table.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thank you Aaron.

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

This is Peter Kaufman, I missed one little factor that is going to be important, suppose that I'm a vendor, which I am, and I want to trust a provider who is given a supposedly trusted identity, you know, out in California somewhere, who is it that evaluates the trust of that other provider's trusting agency? Is it us that my company has to look through all the different frameworks and make sure that, you know, we have to trust them all ourselves or is there an authority that's doing that and once it comes with that stamp we're done, we don't have to do anything further?

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

So, is that a question on that?

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

Yes, that's a question, who is it that does the evaluation of the different trust institutes to determine whether that framework is something that we're...that this identities credential is something we're going to accept from our company.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

You're talking about the trust, who establishes the trustworthiness of the Trustmark provider?

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

Correct, that my company or a hospital, or whoever wants to validate a credential would have to...I mean, are they going to...is somebody...are each entity, hospital, vendor, whatever going to have to go out and do this evaluation and look at the answers to the questions that you showed earlier for each of the institutions...

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

I got you, yeah.

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

Or is it something where there is going to be an imprimatur on it that comes from the government and if it's got that on it, you know, you don't have to go any further?

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Yeah, so let me talk about this just in something that's...a model that's similar, really that's in the private space, if you look at PKIs that are out there today the relationships...and we're actually building a legal framework around this as well, it's really similar to a PKI.

So, in a PKI you have a certificate authority, let's say VeriSign, that does some due diligence with a well defined policy and they vet either end-users or they vet let's say websites, okay, so they go and they vet Amazon to make sure Amazon really is what it is. They have policies, procedures and an agreement that when they issue this certificate, this digital certificate to Amazon that they will, you know, protect the community in a certain way that they will do certain things and then they can assert that certificate on their website to create SSL web connections.

So, that third-party did the due diligence to make sure they actually were issuing it to Amazon. They sent, you know, legal framework that Amazon could assert on their website for SSL purposes and then end-users, in this case, we'll just use that, they have their web-browsers and in the web-browsers there is a list of certificate authorities that they trust and so when that end-user connects to the Amazon site and a little key comes up all is well and they're happy.

And if they don't trust that third-party, that particular third-party, you know, VeriSign, this thing, then a little box pops up and says, you may not want to trust this certificate, you may want to follow this link and do some extra due diligence.

Well, imagine for a second that same kind of relationship exists, that there will be trusted third-parties, not necessarily governmental but trusted third-parties, that are in the marketplace that would assert more than just, you know, the certificate for a website. They could make assertions about lots of other aspects in terms of whether these people actually are doctors that work at these locations or patients, or all the kinds of aspects that you need to agree on in an ecosystem to facilitate HIE in your case or the movement of law enforcement information, or so forth. It's that same kind of relationship.

So, no, the end-user or the end organization or every hospital in this case would basically say, who do we trust as a trusted third-party and it might be for the sector there is a handful of trusted third-parties out there that do this kind of work, they do...and the assessments they hand out the...it could be the government, and they hand out those mini-certifications and the tooling basically...they're put in a registry and then that hospital would say, hey, in order for us to transact we feel comfortable with a certain Level of Assurance and they pick the certifications, they put them in a bucket that they need and they also pick the certifying bodies, the third-parties that they trust and that creates their framework.

It's the same thing that kind of happens today with a monolithic framework except for monolithic framework typically the monolithic framework definer and provider does everything and it is not really suitable for cross sector or for agility as things constantly change.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert

So, this is Scott and I had two comments to make, I appreciate your presentation, John. One of the things that you also run into when you have the scenario in place that you've described that also needs to be addressed for trust to be established, and I think this is the point that was being made earlier, you know, trust is established when trust is earned and often times it's not so much, look we've got the perfect system so you can trust us, we all recognize that we live in an environment where you've got to balance risk versus regulations that you put in place to avoid certain things happening, but we understand that, you know, there are going to be events that nobody likes that are going to happen.

And so one of the things that often I have run into in trust communities that have been established is an important aspect becomes who is going to brokerage any type of dispute resolution that might happen between two parties that are relying on Trustmarks and this is probably an aspect that you're building into your legal framework potentially but...

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Right.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert

That is a key element that needs to be addressed in terms of if you're going to rely upon these Trustmarks if there was a breakdown somewhere whether it was actually in the qualification for the Trustmark in the first place or whether it was in the subsequent use and reliance upon the Trustmark. There needs to be some type of dispute resolution aspect that needs to be taken care of in order for that trust to be able to be established.

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

You very...yes, that makes a lot...you're exactly right and you're right that this is being put into the legal framework and it's modeled after what happens today with certificate authorities in the marketplace issuing, you know, digital certificates so it's the same kind of relationships.

And where a digital certificate points to a certificate policy that's published that defines the constraints of use and responsibilities of that digital certificate and the bounds that's exactly how a Trustmark works. It's an assertion about something different points to a Trustmark policy that defines the relationships and the bounds of use and so forth.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations - DigiCert

Right and so then the other aspect that I also wanted to raise related to that, you know, you had a diagram of, you know, we started out and we had all this data in silos, and then we used to move to federations and so your silos got bigger and essentially, you know, what you described here in my mind is moving to even...it's still even a bigger silo basically, it's broader and it's wider but at the end of the day if you have a number of these Trustmarks somebody, you know, let's take a hospital for instance, has to decide that, you know, what is the set of correct combinations of these Trustmarks that we want to accept to business and generally, again, I'm just going to go from my own personal experience in participating in a number of different trust frameworks, if you give somebody who is an operator within the system needs to make more than, you know, three decisions at run time then you're not going to be very successful.

And so, you know, you gave the example there of, look the web PKI where, you know, browsers have a set of trust anchors that are in there and if you're not in there then you'll be prompted and you have to do your own due diligence, you know, essentially an organization is going to have to establish that set of Trustmarks and combinations of Trustmarks that they're willing to accept, and not a lot of the organizations are well equipped to do that they still need help and assistance in determining whether their specific set of combinations, if you like, which gives them the flexibility to be able to draw from Trustmarks from multiple trust communities, but it might not establish the end goal which is the trust because maybe they're putting them together wrong and it doesn't really accomplish what they were hoping to in terms of trust.

And so, you know, who is expected to provide the organization some type of guidance around, hey, this combination of Trustmarks does establish what you're looking to achieve in terms of trust and if it doesn't have that...

John Wandelt, MS – Division Chief, Information & Enterprise Architecture Division (IEAD) Executive Director, National Identity Exchange Federation (NIEF) – Georgia Technical Institute (GTRI)

Yeah, that's a good point, so how we expect that to happen is that for example you look at a group like the IDSG. IDSG would publish, you know, here's a library, it's almost like in NIEM lots of data components that are out there, lots of different ways you can assemble those together, but for publishing in this case a national rap sheet a community got together that represents, you know, how national rap sheets are sent through all 50 states and they said, here are the components you put together and that's a standard.

And I imagine the IDSG is going to say, here's a set of components for this business context and then to our law enforcement FACA they are standing up and say, here's a set of components that represents our recommendation for best practice for sharing criminal intelligence information across states and federal, and so forth, and that's the set of components that you need. And in those two contexts a lot of those components will be the same components but not the exact set.

So, I see that communities, you know, will get together by some, you know, whether it's through a set of committees or so forth they would assemble that set. The good news is that committee won't have to do all the work. They can reuse things that someone else did that's one of the challenges under the global FACA that we ran into they got into a situation where they started to invent something and then they invented more stuff, and then some other groups outside of the FACA were building things that were close to what they were doing but they had no way, easily way of pulling that in and wrapping it so it would work with what they have. So, they invented new things.

And so there are lots of groups and lots of communities doing a lot of the same things you start to look at overlap between those trust frameworks but because they don't have a model for capturing that and seeing how it relates you find...people are just building more overlap and doing things in different groups that are very similar.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Okay, thank you, we have come to the end of our allotted time and I want to thank John for his presentation and I want to thank the rest of you for dialing in today and for committing your time to this Workgroup. I guess at this point...at the end of every meeting we have time for public comment and since we're right up to 10:30 my time Michelle would you like to open it for public comment?

Public Comment

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

Sure, Dixie, I just want to note that we actually didn't get to review the work plan today so just as a reminder to folks the next meeting is on October 8th and we're planning to have another presentation, but with that we'll open to public comment. 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

It looks like we have not public comment so thank you all for joining and again we appreciate your participation and the next meeting will be on October 8th.

Dixie B. Baker, MS, PhD – Senior Partner – Martin, Blanck & Associates

Thank you, thank you all.

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

Thanks, everyone.

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

Bye everyone.

M

Thanks everybody.

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

Thank you.

M

Have a great day.