OASIS & WEDI Conversation on Cloud, Privacy, Healthcare

17 Sept 2013

OASIS hosted an informal, open call in order to a) get a better understanding of WEDI work on the topic, b) discuss where OASIS PMRM, SAML, XACML, and XSPA standards fit, and c) consider next steps if needed.

Attendees:

Carol Geyer, OASIS

Chet Ensign, OASIS

Dee Schur, OASIS

Devin A. Jopp, WEDI

Hal Lockhart, Oracle, OASIS XACML TC co-chair, SAML TC secretary

Leanne Cardwell, WEDI

Lesley Berkeyheiser, N-Tegrity

Michele Drgon, DataProbity

Mohammad Jafari, US Veterans Health Admin, OASIS XSPA TC chair

Peter Alterman, SAFE-BioPharma

Robin Cover, OASIS

Sue Miller, Health Transactions, WEDI member

Minutes

1. Introductions
2. Overview of WEDI work   
   *Sue:* WEDI was formed in 1991 by the Secretary of Health and Human Services (HHS); the focus is on educating the public on HIPAA regulations. The WEDI Security Working Group started in 2000 with a focus on HIPAA security and privacy. Our mission was to explain and talk to the industry about how to implement HIPAA rule. Since then, we’ve branched into other areas including mobile tools and cloud computing. The Federal government has mandated that all agencies move to the cloud.

Leslie: There are many people in healthcare who have responsibility for PHI but have no idea about the cloud. Our goal is to provide plain English explanations for non-technical people, educate them on how to handle PHI in the cloud, how technology can be leveraged. WEDI is not a standards-setting body. Our perspective on privacy/security is less focused on transactions and more on the business issues. Our white paper takes a first stance, and we plan to do more in-depth case study work. This might fit with what OASIS does with case studies.

*Devin:* WEDI advises HHS on where we think the industry is heading. We also provide them with input for future regulations. We do not do standards, but our research gets used in standards setting. . Most privacy and security standards efforts focus more on business cases and less on business rules. The healthcare community (because of compliance laws) needs rules-based security standards. WEDI would like to actively participate in bringing the two together.

3. How does PMRM fit?

*Michele:* PMRM is unique in that it has been vetted for many years in both government and industry sector verticals. Much like WEDI’s effort for the past 14 years, the International Security, Trust & Privacy Association (ISTPA) developed a privacy framework, based upon the global requirements for privacy, with the goal of providing organization to move beyond the requirements and have standardized framework to “make privacy operational”. That is why it was moved into OASIS as the PMRM effort. The focus is on Privacy and how much of Security to incorporate has been debated back and forth during many of these years– so someone who has been involved in the past year can address how much of security is in PMRM.

*Peter:* PMRM is a methodology for evaluating privacy policies. It is a neutral tool that allows you to array the information about these practices in a way that enables others to understand what is/is not protected and what your privacy model really does. For example, the NIST Privacy Committee has put together a policy. PMRM is a tool for examining and unpacking that policy. It’s a very valuable tool for moving services into the cloud, because users are relying on third parties to implement a privacy and security environment. Security practices are part of PMRM, but only as they are relevant to privacy.

1. How do SAML and XACML fit?

*Hal:* SAML is a set of standards that primarily involve the exchange of identity information in a federated environment. SAML includes protocols that let you share information about users’ authentications and attributes. It boils down to enabling the ability to get information held by others. As security folks, we want that information to be strongly vetted and usable for access control.

XACML is the other piece, representing policies that say, “Given the information we have (about the party, data, time of day, etc.), we can decide whether access should be allowed or not.”

Both XACML and SAML were started in 2001. They are mature standards. SAML is used by many organizations. SAML doesn’t care how you use the data, only that you get it. XACML’s uptake in the market has been much slower than SAML’s, because it must be embedded into existing systems.

In 2008, a healthcare group (including the VA) came to OASIS with the idea of creating XSPA. They had detailed privacy requirements that had been developed in HL7 without reference to XACML or SAML. They wanted to see if these standards could be used to meet their requirements. So they created a SAML profile to define how you access the attributes and an XACML profile about attributes for allowing access to healthcare records. A Profile of WS-Trust was also developed by the XSPA folks to obtain SAML assertions in that way. We developed detailed scenarios and demonstrated them at HIMSS and other conferences. All these materials are available in the OASIS repositories.

We’d be pleased to work to define additional requirements or refine the work that’s already been done.

1. How does XSPA fit?

*Mohammad:* XSPA develops profiles for a protocol used in securely exchanging healthcare data. The current TC is ramping up to address changes in the marketplace. IHE provides a standard for exchange that XSPA is currently considering to align with. There is renewed interest in developing new profiles for specific use cases. There are some crucial gaps that need to be addressed. HL7 has already developed meaningful healthcare appropriate vocabularies, so there is no need for XSPA to reinvent the wheel. HL7 is also developed security labeling.  There is also a trend towards new communication protocols, other than XML. The XSPA TC has decided to only focus on things that are missing, actually on the policy side. We are considering extending IHE profiles, with a focus on evaluating new use cases and developing a security vocabulary for these use cases. We’re studying what’s going on in other SDOs and charting our course.

*Michele:* What’s driving the interest in extending the HL7 vocabularies?

*Mohammad:* We are not extending HL7 vocabularies, but we are considering extending the IHE XUI. There are use cases that the current spec doesn’t cover. XSPA wants to contribute to that and develop some of the extensions that are needed. It’s not the job of XSPA to develop non-security vocabularies.

*Michele:* How do WEDI inputs relate to the NIST cloud specs?

*Leslie:* As we work through the white papers, we use NIST work often. I’d like to say we’re in concert, but the NIST piece we found is much too technology for our audience.

*Sue:* NIST hasn’t come to a definition of what cloud is. Our next step at WEDI is to explain everything that’s out there. Maybe WEDI could also explain what OASIS does in a white paper.

*Hal:* I wrote an article for a healthcare journal in 2008 that provided a laymen’s view of the work. You might find it helpful.

Note that the SAML and XACML TCs don’t have the ability to vet requirements that are brought to us. We can’t say how much of the healthcare world we’ve addressed or what overlap there might be.

6. Is there a need for a new standard or a profile/extension of existing standard?

*Sue:* WEDI is constrained by what it does. We deal with HIPAA regulations. That doesn’t necessarily mean we wouldn’t participate with OASIS. We could continue the conversation, we could survey the industry, but we don’t have the technologists.

*Leslie:* People who follow WEDI want practical assistance on where their data is, they want to know what tools are recommended and how to safeguard their information. Obviously, standards-setting needs to occur, but awareness and keeping data safe is our focus. We speak to business users not technologists. We work to raise levels of awareness.

Chet: Is there anything unique about the business requirements of HIPAA that aren’t covered by existing standards, or is it too early to know that?

*Sue:* The HIPAA Privacy Rule is a use and disclosure regulation. I wonder if there might be a meeting of the minds there. Privacy is policies, procedures, templates to do the work.

*Michele:* Whether it’s a standard or white papers, do you think that Omnibus is something that needs to be augmented in PMRM? Could OASIS use WEDI’s help for this?

*Sue:* Omnibus rules are social changes (e.g., asking to have your information restricted at your doctor’s office), but there are some things that could be part of a structure--specifically access, accounting for data, amendment. The industry is certainly going to need help with accounting for data.

*Michele:* WEDI has valuable insights that could be translated into use cases for PMRM.

*Peter:* I think PMRM is sufficiently abstracted. You have to apply the template to each particular use case. There isn’t any larger conceptual model that’s been adopted. It’s a use case environment. So PMRM has to be applied to each particular use case. PMRM is mature enough to be a useful tool.