**Global Federated Identity and Privilege Management (GFIPM) Initiative**

The following is the first of a series of podcasts on justice information sharing national initiatives for 2009. These podcasts are presented by SEARCH, The National Consortium for Justice Information and Statistics. This series is made possible through a grant from the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

Today’s topic is the Global Federal Identity and Privilege Management initiative. Justice organizations are looking for ways to provide secured access to multiple agency information systems with a single log on. The GFIPM initiative provides the justice community with a security and information sharing architecture that is based on an electronic justice credential. This standards-based justice credential can be used to securely connect law enforcement and public safety personnel to enter agency applications and data over the Internet. Our guests today are John Ruegg, Chair of the Global Security Working Group and Director of the Los Angeles County Information Systems Advisory Board or ISAB. Also joining us, we have James Dyche, Applications Administrator with the Pennsylvania Justice Network or JNET.

I’d like to start today’s podcast by noting a few recommendations made by the Global Advisory Committee. The first is to recognize GFIPM as a recommended approach for developmental interoperable security functions in authentication and privilege management for information exchange. The second is to urge the members of the justice community to consider GFIPM as a potential building block to a layered security solution with authenticated users among cross-domain organizations.

Interviewer Jim Douglas: Good morning, John. Based on these recommendations, could you provide our listeners with a description of GFIPM.

John Ruegg: I think the easiest way to understand it is in today’s Internet world, we require user name and passwords to multiple information systems at our work or bank or online shopping, airline accounts, and we provide each of these external systems our personal information or credit card information, lots of personal information and lots of different systems. The Global Federated Identity and Privilege Management program is a new business model where you provide your identity and personal information to an identity provider information system and that identity provider system will you connect you to multiple external systems on your behalf. You will have a single sign on, your identity provider will protect your information and shares only the information that’s required by those external systems to determine if you’re authorized to access those systems. So, these external systems that communicate with your identify provider, we call relying parties and a collection of these identity providers and the systems you can get to these relying parties form what we call an identity and privilege management federation, and we call that program the Global Federated Identity and Privilege Management standard. So, in a nutshell, GFIPM is about establishing your identity with a single identity provider and letting that system communicate with all the other systems instead of you having to log on to multiple systems or provide your personal information to all these different systems.

Interviewer Jim Douglas: Thanks, John. As a follow up, how does GFIPM define a federation, and what is the relationship between a federation and trust?

John Ruegg: We define a GFIPM federation as the set of technical standards, policies, and procedures for sharing identity and authorization information among the federation partners. As I described a moment ago, you’re going to have an identity provider that’s going to authenticate you and keep track of your identity information and then you have the other federation partners who are going to rely on that identity provider to provide that information. So, the technical standards and policies and procedures for accomplishing that is basically what a federation—a GFIPM federation is. In terms of the relationship of a federation to trust, there are really two components of trust. The first step is you want to ensure that any member of your federation is a reputable, reliable legal entity, which you do business with and that involves qualifying that organization for joining your federation. So, that component of trust is kind of a management organizational contract and we’ve developed a guideline for establishing that organizational trust called the GFIPM Governance Guidelines and then what your responsibilities would be as a federation partner, either relying partner or an identity provider, we’ve given the overall responsibilities described in another document called the GFIPM Operational Policies and Procedure Guidelines. So, that’s the first component of trust is deciding which organizations you are willing and you trust to do electronic information exchange with. The second component of trust is really an agreement to follow a prescribed set of technical standards for ensuring that secure electronic information exchange of the identity attributes and the privileges attributes between the members of the federations. So, that’s more of a technical standards and trust that those standards will be followed in executing secured information exchange of identity information, the personal information, and the attributes necessary to make these authorization decisions in the federation. So, there are two things that make up the trust within a federation and those are them.

Interviewer Jim Douglas: Hey, James, would you like to follow up?

James Dyche: Just as far as adding to, I think John did an excellent job of really talking about what a federation is and the relationship of the federation and trust. I want to go back maybe just to kind of maybe in a little more layman’s terms and some of this may come across more from a business prospective, but when you look at a federation, it’s really the union of autonomous Global partners or justice partners who are uniting themselves together for some basic reason and the basic reason we’re finding ourselves in with justice is really the sharing of information and particularly in GFIPM, we’re sharing identity information. This is all being done so that we can securely transmit justice-based information. So, the federation, I think, in a layman’s prospective might be more a union of these justice partners. As far as the relationship between federation and trust, I kind of look at federation as really what brings us together and a trust is what gives us the confidence to enable the sharing of the information and the confidence we’ve had in the past is really around identity information and where we’re getting it from and how we get it. So, I know today’s more typical business is thought of as entrusted VTN connections for private networks and is just an older—is really becoming another way of doing business. From the aspect of private side, we would trust that the traffic that’s flowing on those networks and in the past, you know, we built these back in trusted processes between business partners and how they vet their users. We will do that before we hook up that organization or agency through some sort of VTN or more secured connection. But the beauty of the federation that we’re going to talk about here with GFIPM is it really uses the latest set of encryption standards to protect the data, but it really no longer requires the use of these privatized networks. It allows us to do this in a little bit more open architecture or infrastructure, and as John had said, the comprehensive policies are really the guidelines that enable us to manage that risk and provide the foundation for trust. Maybe an example of this, and we’ll get to this example—maybe use this a little bit more is JNET, who is an organization here in the state of Pennsylvania, might want to trust some information from RISS, which is the Regional Information Sharing System, and the fact that we have a user in one of those systems, we have a level of confidence of who that person is based on the attributes that John referred to and what they should be able to see from a provider prospective.

Interviewer Jim Douglas: James, you mentioned the use of secured privatized networks to securely transmit information and the transition now to using open standards to create these trusted networks essentially across the Internet. Could you talk a little bit about the open standards and the technologies being used by GFIPM to establish these trusted networks.

James Dyche: There are really a number of standards which were used in bringing the GFIPM proof of concept into an actual live environment. SAML, which is the security assertion markup language. This is an OASIS standard that defines XML-based standards for data authentication and authorization between disparate security domains. This includes the providing of any of the attribute information to enable the authorization process. That will probably be one of the larger standards that we use in the industry for the solution. XML, which is the eXtensible markup language, was also used quite extensively for us in enabling the attributes sets that were passed. All of this particularly takes advantage of the TCPI, which is the basic network protocol, sometimes known as the Internet protocol suite and that protocol is basically essential for this whole solution to work. Along with the HTTP and TTPS, which is the hypertext transfer protocol secure and that can also be run in different layers. There’s secured using the secure socket layer or intransport layer security. Transport layer securities is the newer security mechanism we’ve been using to protect the data that is moving. A couple of other standards that we’ve used LDAP and LDAP-S, which is a protocol used for querying and obtaining information from back into directory stores. Then we have NIEM, which is the National Information Exchange Model, which is a more of a justice-based standard used to provide common semantics for the information that we’re sharing. Those are pretty much a number of the industries standards that we’ve used to enable this solution. For the original pilot, GFIPM effort a proof of concept effort, we did put together an open-source solution that used a number of open-source technologies. They include the Shibboleth project, we started with Shibboleth 1.0, and the concept was later migrated to Shibboleth 2.0. That’s probably one of the more core open-source projects that was used to put together what we’re going to talk about a little later in the identity and service provider aspects. That also uses Tomcat and Apache from an open-source prospective. I know that there are also a number of other commercial companies that provide federation and security solutions. Some of the ones that I’m aware of—and not all of these have been implemented yet but are involved with the GFIPM concept—include the Ping Federated Product, Computer Associates SiteMinder, federation security for SiteMinder, the Kogelson Trusted Broker Solution, and IBM Data Power. And, again, there might be others there that are also looking into enabling GFIPM, and I would encourage the justice folks to reach out to IJIS for more of an industry list in the security aspect.

Interviewer Jim Douglas: John, what is the relationship between GFIPM and other information sharing initiatives, such as the Global Justice Reference Architecture and the National Information Exchange Model or NIEM?

John Ruegg: The JRA defines a complete technical model and a set of components for developing secure information exchanges and the GFIPM addresses a subset of all of those JRA components by specifying standards specifically for federated identity access management to information services. But you’ve got to realize that these specialized identity and privilege management capabilities—things like identity providers and relying parties and security token services, etc.—the way we’re implementing those is we are implementing them as complete JRA services. So, really GFIPM are just specialized types of services specifically deployed as a service between you the service requester and the information you want to access but the GFIPM model sits in the middle, because the services—what they do is what they have kind of traditionally done—is they determine before you get any information, that we know who is requesting the information, we know attributes about that person, and we authenticate that person, and all of that needs to be completed before the service provider relinquishes any information for an information exchange. So, really, GFIPM performs the security functions in a federated model and the JRA addresses the security functions as a piece of your whole services specification for the actual content that you are exchanging—your justice information that you are exchanging. But in all exchanges, that layer, that security layer, which GFIPM specifically addresses, sits as not a barrier but a level or area that you need to get through before you can participate in getting a successful information exchange.

James Dyche: So, just to follow up with John’s response on the relationship between GFIPM and the JRA, I think it’s important for the folks to understand there is a clear business relationship between these particular entities. Just to start off with, all these efforts were at one time or are currently under the direct supervision of Global as far as a leadership and the business owning entity. Global for those that are not aware is a federal advisory commission that was established to provide advice to the Attorney General on various justice issues. So, from a relationship, I would say that Global is kind of the parent organization of JRA and GFIPM, and they are kind of children to each other and John, who is on the phone with us today, is the Chairman of the Global Security Working Group, where GFIPM fits from an organizational prospective, and JRA is under the direction of Global Infrastructure and Standards Working Group, which is Chaired by Dr. Tom Clarke. Both of these entities are working closely together to ensure that the frameworks that are being put together will interoperate together.

Interviewer Jim Douglas: And, John, as a follow up, how do the Global privacy technical framework and GFIPM fit together?

John Ruegg: Well, in GFIPM, the requestor of a federation service involves your identity provider presenting a set of attributes to the federation service you want to access. The federation service uses those GFIPM attributes and a set of authorization rules to determine whether they are going to grant or deny access and to determine what information that they can provide you, based on your GFIPM attributes. So, what the Global privacy technical framework describes is the open-standards and the commercial products that can be used to develop electronic authorization rules that comply with the written policy and access rules of their particular service provider. So, the service provider always controls the access to their resources, based on evaluating the requestor’s attributes or claims. So, the focus of the Global technical privacy framework is really taking your current security and privacy policies in written form and using tools to author a set of business rules using open standards, to make that access decision as to whether you are granted or denied access to the particular resource that they provide.

Interviewer Jim Douglas: Thanks, John. James, GFIPM refers to an identity provider or IDP and a service provider or SP. We’ve talked about these two entities a little bit already, but could you explain what each is and their relationship.

James Dyche: Sure. An identity provider and service provider really are the two main roles that a federation partner can perform while in the federation. The federation partner does not really have to set up or perform both roles. From a high-level IDP prospective, it’s really about the partners’ users that they are providing to the federation, and the service provider is really about the partners’ content and what type of applications they are bring to the federation. So, it’s typical that a partner does eventually perform both roles, however, it’s really not required and that they may provide one role or another depending on if they are interested in providing content or expanding the content for their users by providing their users to the federation. So, from a business prospective, just looking at the identity provider, this is really one of the core mechanisms used to enable entity attribute sharing in the federation and an IDP is typically comprised of hardware and software that provides the functionality between your trusted partners with basically your internal directory of users as provided and shared with the federation in a secured way. The service provider from a business prospective really enables you to provide the content that you have in sharing that with other partners in the federation. The SP role that the partner may need to have or get to provide information from a broader set of users than really what it has, and this way provides them a mechanism to access a larger community than they might have within their own purview. So, as far as the relationship between the IDP and the SP, they really work hand-in-hand, even though it’s typically two distinct partners’ perspective. In other words, for example, we have JNET law enforcement officer that attempts to access the RISS or Regional Information Sharing System. RISS would ask the user to identify their home location, and that user would be redirected to their home location where they would authenticate using their normal credentials using their JNET credentials and then their attribute information will be passed back to the RISS service provider. The RISS service provider would be provided with a full set of attributes, it would understand whether they are law enforcement officers, whether they are certified under CFR 28, and then RISS would make the decision of the information they would provide to this trusted user. And, again, I want to reiterate what John had said earlier, the final decision for providing information fully rests on the service provider’s side.

Interviewer Jim Douglas: Thanks, James. And John, could you provide our listeners with some of the benefits of using GFIPM for authentication and authorization for information access.

John Ruegg: Well, I think that one of the things we have to recognize is that employees change job roles. Here in LA County, our law enforcement change job roles about every two years. And the systems that they access change when they change job roles. In using a GFIPM model, instead of the traditional model of registering with a whole set of systems and then when you change jobs, getting deregistered from those systems and getting new user IDs and passwords for a different set of systems. In the GFIPM model, it only would require that the employee get his information updated through his identity provider and then all the federation systems are always getting current identity attributes about that employee, and they always make the access decisions based on those attributes, so when you change job roles, everybody knows about it. You don’t have to re-register in all these different systems for that to be current and update it. Also, users can enjoy a single sign-on process by participating in a federation, because the identity provider is doing all the access attributes and is sharing those among all the partners so you can support the single sign-on. There is also opportunity for some privacy or anonymozation of your identify. You may be very authorized and entitled person to a number of systems out there, but you really don’t want your identity known. So the law enforcement agency has people that work undercover, etc.. For an identity provider, they could provide because the federation trusts the identity provider. They could provide information about that individual without actually disclosing his name, badge, address, etc., like that. So, that’s another functional thing that you could do in this environment. It’s very difficult to do in a nonfederated environment. This identify provider for your organization could be used to provide attributes to other federations. So, once you have this infrastructure in place and other federations are coming on board in terms of following these kinds of federated standards, you get a lot of reuse out of this function. I guess the other thing that is really important is by having an identity provider in your organization, you have better control over having current attributes on your employees instead of each division filling out forms and registering with all these external systems. Everything is being managed by your central identity provider and that makes for more accurate information and more current information for all of the members of the federation. So, in a secured federated model, you don’t need to register into multiple systems and your information doesn’t become stale-dated in all these multiple systems, because you don’t have to deregister yourself, either. So, I think there are a lot of advantages to this model of doing business, provided you follow the standards and you establish the appropriate business relationships and governance model to make sure everybody trusts, with that old factor of trust again, that everybody is doing their part either as being an identity provider or a service provider.

Interviewer Jim Douglas: James, could you talk about the background and the current status of the GFIPM operational pilot in which JNET has been a participant.

James Dyche: Sure. Let me start maybe by providing a little bit maybe by a timeline just so our users understand how long this particular project we’ve been working on is. Back in 2005, there were a number of folks who got together and recognized some of the security challenges that we were facing across the justice practitioners set. John had alluded to single sign-on as in GFIPM provides that functionality today. Unfortunately, most of us do not have GFIPM enabled and are dealing with a lot of the issues that come by not having a single sign-on-type solution. Users are managing multiple user IDs and passwords. They are dealing with renewal processes of those passwords every so often, whether that’s three months, six months, a year. There are dealing with security forms to register to get access to new systems. A lot of challenges in this area. Admin time of officers being spent, instead of being on the street and practicing public safety, dealing with administrative things to provide them access to systems themselves. So, again, this was discussed back in 2005, and a concept was put together under the direction of the Homeland Security folks and a grant basically awarded to Georgia Technology Research Institution to help provide some more structure to an approach that might resolve a number of these problems. Around the second quarter of 2005, there were three partners that joined in on this grant and that was the Pennsylvania Justice Network, the Regional Information Sharing System (RISS), and CISAnet, which is a criminal information sharing alliance. All of these were pulled together to pilot the concept of a trusted federation. The infrastructure was deployed basically beginning in 2006. Most of 2006, we spent a good bit of time trying to get the technology sets pulled together to enable these technologies and the federation to be able to talk one with another. About late 2006, we were able to put together the actual solution to demonstrate the movement of information through this system. In 2007 or so, JNET actually invited the FBI in for an audit. We had a lot of questions from the FBI and basically met with them to show how we could eventually put together a complete audit trail with the solution to enable auditing of the user credentials that are moving and again, had a number of discussions with them. At the end of 2007, there was a full project report put together, which was the GFIPM Security Interoperability Demonstration Project. It’s a very lengthy document that was put together in early 2007. That report really provides a full set of the findings from the pilot project, and it was officially published in August of 2007. We will talk about the Web site in closing comments where some of the listeners can get a hold of these documents. In 2008, we really spent coming back and readdressing the foundation of getting policies and finalizing and kind of wrapping the solution. They did a lot of the work there and additional agencies were on-boarded during this time. The DHS-HSIN project was on-boarded along with a couple of other agencies in 2008. I would say that 2009 has really now been about more reviewing and finalizing the policies and procedures that go along to really provide that trust and the relationship between the federation and the trust. One other point of note is the CONNECT project is a project that is successfully using GFIPM now in more of a services approach for moving drivers’ photo and demographic information in a trusted way between systems. This is a new usage of GFIPM or of a service-to-service-based concept of GFIPM and will be more of how the JRA ties in with this solution for the future.

Interviewer Jim Douglas: And gentlemen, I would like to give you an opportunity to provide any final comments you may have for our listeners regarding GFIPM.

John Ruegg: I would just like to say that federation industry standards, standards for authoring policies or authorizations services and identity management tools are available in the commercial market right now from all of the major venders, including IBM, Oracle, and Microsoft. The trend in industry is toward moving to a federated model for identify management and authentication of users and authorization software and pulling that out of the line of business applications and managing security and policy functions and services that interface with applications. This approach removes the burden of interpreting policy and law by software programmers, which is what we’ve done traditionally. Every line business application has figured out what the real authorization policy would be and encoded in their application, which makes it difficult to update, difficult to correct, and difficult to manage. With the specialization of putting security outside of the applications, we really start shifting the responsibility back on the business policy people to modify, update, and keep policy around what information resources you can access, secure and consistent across the enterprise. So, I think Global, GFIPM, and JRA provider roadmap for achieving that kind of interoperability by leveraging the open standards that our industry partners are also adopting.

James Dyche: I’d really like to encourage all our government and justice agencies that are out there to really consider becoming part of the GFIPM trusted user federation. For really a lot of the benefits that have already been discussed throughout this podcast, the justice integrators that are out there, I would really encourage them to become more familiar with the solution and understand what it means. As John talked about earlier, the industry is definitely adopting this and moving a lot of the commercial industry forward, and I would encourage the justice integrators to look more in depth at the documents that we have and will provide on the Web site. I also want to encourage them to spend some time looking and digging into the technical documentation so they better understand how the GFIPM solution is implemented and how they might be able to then determine how they provide these solutions to their partners and clients. Another thought, as far as closing, is to really think about how this solution could improve your business, either in expanding your business base or by providing information that you have to a broader user base that you’ve not been able to reach or get to in the past. There are a number of resources that are available around GFIPM, and I would encourage you to hit [www.it.ojp.gov/gfipm](http://www.it.ojp.gov/gfipm). This will provide you with information on the standards and the policies that were mentioned earlier in the podcast. I also encourage you to hit gfipm.net. This particular Web site will give you more information around the security interoperability demonstration that we discussed as far as the history of GFIPM.

Interviewer Jim Douglas: And, gentlemen, I would like to take this opportunity to thank you both for participating in this podcast.

James Dyche: Thank you, Jim.

John Ruegg: Thank, you, Jim.