Virtual WG Chat Transcript

Virtual Working Group Chat Transcript

A social identity virtual working group meeting was held on May 20–21, 2013. The transcript of the real-time chat conversation recorded during the webinar is pasted into the panel at the bottom of this page. A refactoring of the chat conversation, in question-and-answer format, follows:

Q: Does the Google OpenID Gateway assert `eduPersonPrincipalName`?
A: To our knowledge, no social IdP asserts a true scoped identifier like `eduPersonPrincipalName` (`ePPN`). However, the Google OpenID Gateway may be configured to compute a value for `ePPN` based on the user's email address (`user@gmail.com`), which is known to be a stable attribute for the user. Currently, one of two `ePPN` formats may be configured:

1. `user@gmail.com`
2. `user+gmail.com@gateway.incommon.org`

Other `ePPN` configurations are possible but a basic issue remains: what scope value(s) are asserted in IdP metadata and will those scope value(s) be accepted at the SP? There are no easy answers to these questions. See the wiki topic Google OpenID Gateway Attributes for further discussion.

Q: Does the Google OpenID Gateway assert `eduPersonTargetedID`?
A: Yes, the Gateway will compute a value for `eduPersonTargetedID` (`ePTID`) in addition to `eduPersonPrincipalName`. Fortunately, we have a better story for `ePTID`. Google asserts an identifier called a *Private Personal Identifier* (PPID), defined by the Federal ICAM OpenID 2.0 Profile (which the Google OpenID IdP supports). As it turns out, a PPID is a great fit for `ePTID` since both are targeted (per-SP) privacy preserving identifiers. See the wiki topic Google OpenID Gateway Attributes for examples.

Q: Does the Google OpenID Gateway run an invitation service?
A: No, the current version of the Google OpenID Gateway does not include an invitation service. This has been discussed, and some have expressed interest, but no one has proposed a reasonable method for transmitting identity information from the Gateway to the campus.

Q: Does the Google OpenID Gateway persist user attributes or identifiers?
A: No, the Google OpenID Gateway is a stateless gateway. Depending on how you configure the Gateway for `ePPN` and `ePTID`, the Gateway can function as a 100% passthru gateway. It is extremely lightweight by design.

Q: Is the metadata for the Google OpenID Gateway included in the InCommon metadata aggregate?
A: No, there is no metadata in the InCommon metadata aggregate since the Google OpenID Gateway is currently a beta deployment. Once the Gateway reaches production status (by the end of Q2 2013), metadata for the IdP component of the Gateway will be submitted to InCommon.

Q: When the metadata for the Google OpenID Gateway is finally included in the InCommon metadata aggregate, will any InCommon SP be able to use the Gateway?
A: Initially, only Internet2 and InCommon Operations will be able to use the Gateway. Once a funding and support model is determined, we will scale the Gateway to additional participants.

Q: Assuming the Google OpenID Gateway is ultimately rolled out to a large number of InCommon participants, are there concerns about metadata explosion?
A: No, the architecture of the Gateway requires a single IdP in InCommon metadata. In that respect, the "Google Sign In" IdP is no different than any other InCommon IdP.

Q: To use the Google OpenID Gateway, what modifications does an SP need to make to its metadata?
A: No changes to standard SP metadata are required to use the Gateway.

Q: What if Google decides to join InCommon in the future? Wouldn't there be two Google IdPs in metadata in that case?
A: Yes, it's remotely possible that Google itself might want to submit IdP metadata to InCommon in the future. If that were to happen, the `entityID` of the IdP would have to change, so for all practical purposes the two IdPs would be distinct (and of course the DisplayNames would have to be different). Even if Google did join InCommon, it's doubtful Google would be willing to assert **any** eduPerson attributes. If you're concerned that Google might join InCommon and break your deployment, the best thing you can do is ignore the eduPerson attributes asserted by the Google OpenID Gateway and rely solely on the user's email address.

Q: Is there a level of assurance associated with the Google OpenID IdP?
A: A handful of social identity providers are certified by OIX to be US ICAM LoA-1 Certified Identity Providers. (Like InCommon, OIX is an ICAM-approved Trust Framework Provider.) In particular, the Google OpenID IdP is a certified ICAM LoA-1 identity provider.

That said, the Google OpenID Gateway does not assert any particular level of assurance (LoA) value (unspecified); it just echos the attributes that Google provides and computes a couple of its own (`ePPN` and `ePTID`). Nothing can be said about the trustworthiness of these attributes, which are not covered by any InCommon Federation policy. Thus service providers must make their own determination regarding LoA on a per-transaction basis at their own risk.

Q: What is this thing called a "realm" that appears on the Google consent page?
A: A *realm* is strictly an OpenID construct (there is no such thing in OAuth flows). In a Google OpenID flow, the realm is synonymous with the hostname of the OpenID endpoint at the RP. Google uses this hostname in the same way SAML IdPs use MDUI SP DisplayName.

Q: Does the use of the Google OpenID Gateway violate Google's license agreement?
A: The short answer is no. If there were any chance we might be in violation of some license agreement, we certainly wouldn't be advocating for a central gateway service. The risk would simply be too great.

The architecture of the Gateway forces an administrator at the campus to enable and configure the Gateway for each SP. Neither InCommon Operations nor Cirrus Identity is involved in this configuration step. Thus the campus assumes any and all responsibility for accessing and utilizing the Google OpenID IdP.

Q: Does the Google OpenID Gateway run a discovery service so that the SP doesn't have to?
A: No, the Gateway does not run a discovery service. Such a service would be a centralized discovery service by definition, but InCommon already runs such a service so another one would simply be a duplication of effort.

Real-Time Chat Conversation

Dean Woodbeck:Audio is available via Adobe Connect. But to participate in the discussion, you will need to use the phone bridge for audio (if doing so, please mute your computer speakers): 734-615-7474, or 866-411-0013 (toll-free in US and Canada) PIN: 0157272#
David Langenberg – uchicago:yes
Tom Scavo:I can hear you!
Daniel Yu(UofC):yes
Mark "Max" Miller:Sounds good!
Dean Woodbeck:Slides are available on the wiki: https://spaces.at.internet2.edu/x/NYBHAg
Tom Scavo:Dick Visser (TERENA) is a pioneer as well.
Tom Scavo:Any SAML service provider software should work (not just Shibboleth)
Nathan Dors:doesn't AITOawmLuj.....etc break the usability requirement?
Tom Scavo:@Nathan Not all use cases require an invitation
Tom Scavo:Spaces, for example, needs an "Identity Provider of Last Resort," which the Gateway provides
gettes:@nathan what "username" is passed to the SP remains an interesting question. The junk you see is the openid username passed by some providers - like google. the gateway could translate the username into something per human readable. it brings up the issue of apps displaying username which may not be a good practice.
Nathan Dors:the invitation flow is friendly, like a party invitation. like @gettes says, it's the usernamethat creates the challenge
Russell Beall:We choose to translate the username into a custom identifier @guest.usc.edu. It can be a license plate or chosen by the user.
Nathan Dors:CMU has one too, i think
gettes:CMU currently passes on openid@affiliates.cmu.edu - we are working with cirrus identity and may move to emailaddress@affiliates.cmu.edu (the @ in the email address translated to + or something).
gettes:i will say the openid based username was a great opportunity to teach apps why it is bad to display a username.
Eric Goodman (UC):@gettes
Eric Goodman (UC):🙂
gettes:speak louder please?
keith hunt uakron:why is it a bad practice for apps to display username?
gettes:cuz in a federated world - you won't have control over what that username looks like. there are those who provide 64+ char usernames and it may screw up the screen layout.
keith hunt uakron:I see
Russell Beall:and it would be confusing to the user because they think they are 'customname'@google.com, not the wierd thing that showed up
Russell Beall:customname@google.com, not the weird thing that showed up...
keith hunt uakron:I see that too
gettes:@carmody regarding Grouper invitation service - the user identity only lives in Grouper, right? It's not exposed to your identity management system?
Brown - Steve Carmody:today, the user identity is stored in a a DB separate from our Identity mgmt svc (person registry)
Brown - Steve Carmody:we are in process for deploying a new Person Registry, and I expect we will be creating entries in that for people with social identities
Brown - Steve Carmody:we have a groups deploy project underway right now;
gettes:so, within Grouper, you have the invite service using a different subject source, is that how you did it?
Brown - Steve Carmody:it will be creating user objects in our ldap server for these people, and adding them to groups within our ldap directory
Brown - Steve Carmody:re different subject source, – yes, today it works that way
gettes:bugger. adobe connect just blew chow on my chat - lost most of the messages.
Tom Scavo:More on delegated administration of metadata: https://spaces.at.internet2.edu/x/7ZiKAQ
Dean Woodbeck:@gettes - I'll email you the chat
Dean Woodbeck:@gettes - thanks, too, for the imagery while I'm eating lunch
gettes:@dean sorry about that - i had already finished my lunch.
Tom Scavo:A visual demo of the Google Gateway: https://spaces.at.internet2.edu/x/jAFOAg
Brown - Steve Carmody:https://spaces.at.internet2.edu/display/socialid/Draft+requirements+f or+a+Social2SAML+gateway+service
Eric Kool-Brown (UW):Is there a concern about metadata explosion? How will this scale for shared metadata?
Tom Scavo:@Eric There is only one "Google Sign In" IdP in InCommon metadata (if that's what you mean)
Eric Kool-Brown (UW):Is there addition SP metadata beyond the standard SAML info?
gettes:and what if google really wants to join InCommon? then we have 2 google IdPs? Personally, i think this approach is too complicated.
Tom Scavo:@Eric No, no metadata customization is required at the end SP
Brown - Steve Carmody: "What are the barriers to your institution deploying support for authentication by social providers (twitter, yahoo, google, Facebook etc.)?
Chris Bongaarts (UMN):if google joins incommon, you just switch to a federated instead of gateway model
gettes:not true - the userids will be different.
Tom Scavo:@gettes We would be happy to withdraw the Gateway if Google were to join InCommon 🙂
Denis Hancock - University of Missouri:level of assurance
Brown - Steve Carmody:I don't think anyone is expecting Google tojoin IC at this point
gettes:and disconnect all those users? that doesn't sound very friendly.
Tommy - SMU:What on the IdP side tracks the relationship between the social ID and the "registered ID"?
Eric Goodman (UC):Certainly some sort of (local) policy or guidance around when it's appropriate to use Google IDs (might go beyond LoA concerns)
Eric Goodman (UC):or other social IDs
gettes:@carmody - i don't agree with betting on the future
Tom Scavo:@Tommy Are you referring to the identifier asserted by the Google IdP?
Tommy - SMU:correct
Chris Bongaarts (UMN):perhaps google could be persuaded to release an openID identifier for a user as an attribute
Tom Scavo:The Google identifier (called a Personal Private Identifier) is analogous to eduPersonTargetedID
Tom Scavo:Every SP gets its own PPID for the user.
Chris Bongaarts (UMN):if PPI includes "idp" as part of its uniqueness then my idea would be a nonstarteer
Tom Scavo:@Chris The PPID is converted to an ePTID at the Gateway

Kevin Legget - Northeastern:We currently provide credentials to over 10,000 "parents" and I would prefer to be out of that business. However, I am concerned about the access to certain applications (billing, student bio info, grades, etc.) but I see the potential here.
Nathan Dors:@Tom, is there a wiki page that clearly describes that attributes asserted by Google (email, username, etc) and their appropriateness for SP consumption?
Tommy - SMU:@Tom thanks, but the discussion was that there was an association between the Google identifier and either an existing campus account or one the user signs up for in real time. So what databases maintains that association for the IdP?
gettes:@kevin - yup, that's why we rolled out our S2S gateway
Earl Lewis - UofU:is anyone speaking?
Eric Goodman (UC):Many of the desired use cases seem to involve access to relatviely sensitive data e.g., access to student bills. Are there guidelines /thoiughts around when that's appropraite? (kind of a followup to Kevin's question"
Nathan Dors:@Steven, personally I don't think assurance attributes are a must-have for phase 1
Earl Lewis - UofU:i can hear now
Tom Scavo:@Nathan Let me see if there's a wiki page...if not, we'll start one
gettes:@john and whether or not registering social IdPs in metadata is actually a good idea.
Tommy - SMU:Definitely agree that accounts for parents (over 10,000 of them now) is a big driver for us to move to social authN.
Nathan Dors:@Tom, thanks. we may be able to contribute to that.
Tom Scavo:Google OpenID Gateway Attributes: https://spaces.at.internet2.edu/x/EgZOAg
Michael Hodges @ U of Hawaii:Id like to understand the pros and cons of storing social ids in the person registry
gettes:not on voice - is access to a student bill sensitive?
gettes:we thought not.
gettes:there is no personally identifiable info on the bill. and yes, the student is in control - the authorizer
Nathan Dors:to a particular identifier or to a particular email address?
gettes:no risk to the university in accepting money. 🙂
gettes:we used to send the bills out by email
Eric Goodman (UC):Good point; I think I was thinking of specific systems where billing and records and not clearly separated.
Eric Goodman (UC):are not*
Chris Bongaarts (UMN):applicants are of interest to us as well
keith hunt uakron:do Google et al promise not to track anything about my login to an SP for their own use?
gettes:google promise? funny. what does a google promise look like?
Tom Scavo:@keith Google doesn't know anything about the SP on the other side of the gateway
Chris Bongaarts (UMN):@gettes: "don't be evil" 😛
Loren Frerichs -UNL:in our student records system studnts can add a "guest for thier records" that only that student can reset the password for
Chris Bongaarts (UMN):@scavo in krienke's diagram it would
gettes:@chris - if you have to say "don't be evil" then you already are.
Tommy - SMU:In our case, we allow the student to authorize anyone to have a sponsored account to not only pay bills but also optionally view academic information if they choose.
Chris Bongaarts (UMN):@gettes i actually meant to stick the tongue in my cheek rather than out 😉
Kevin Legget - Northeastern:Does Cirrus expect to have an available GW by early November (the week established for the "Identity Week")?
Chris Bongaarts (UMN):we have a parent proxy setup like tommy@smu
Tom Scavo:@Chris Yes, I suppose SP-specific gateway in the box outlined in blue dotted line is tracked by Google
Tom Scavo:But doesn't any IdP in the InCommon Federation know exactly what services it interacts with?
Kevin Legget - Northeastern:On another note, the URL for the "Identity Week" event on the I2 page is not functional.
Dedra Chamberlin:I certainly hope we will have something ready not just to demo, but as a viable service by November, yes
Brown - Steve Carmody:https://spaces.at.internet2.edu/display/socialid/Draft+requirements+f or+a+Social2SAML+gateway+service
Tommy - SMU:Great topic, and I'd like to hear much more.
Nathan Dors:are the ordered lists ordered by priority?
Eric Kool-Brown (UW):I'm confused about the SP identifier in the consent page. Has this issue been worked out by Cirrus?
Brown - Steve Carmody:@nathan – not prioritized.
Tom Scavo:@Eric We have **a** solution but I don't know if it's **the** solution
Nathan Dors:right.
Keith Hazelton, UW-Madison:I do keep wondering why more campuses haven't started down the path of Social2SAML services. Is it capacity? Lack of a local campus driver?
Dedra Chamberlin:We have had a number of conversations about SP identifier in the user consent page
David Bantz, U Alaska:Lack of capacity to take on more...
Tommy - SMU:We discuss it quite a lot and not sure how best to move forward.
Nathan Dors:yes, lack of capacity. we're deploying this stuff to support social logins to Canvas
Dedra Chamberlin:For OAuth providers, the text a user sees is configurable, and can describe the SP in user-friendly terms
Chris Bongaarts (UMN):@hazel it's definitely been brought up as an interesting idea. part of it for us is OIM project which and related uncertainty
Dedra Chamberlin:For OpenID, the info displayed is tied to the domain
Russell Beall:Is there any more information on whether gateway usage of OpenID/oAuth providers will violate the providers' licence agreements
Russell Beall:Does InCommon have an arrangement with Google?
Tom Scavo:@Russell Using the architecture outlined in the diagram to the right, the end SP is in control of their piece of the Gateway, so there's no need for InCommon Ops or Cirrus Identity to "be in the middle"
Tom Scavo:In other words, we nicely sidestep any legal issues
Russell Beall:So, each SP would have to register with the providers if using oAuth (luckily OpenID doesn't require such registration of a service...)
Nathan Dors:some SP owners have asked if the Gateway will host a configurable discovery service for them too, so they don't need to implement one local to the SP
Tom Scavo:@Russell Exactly.
Tom Scavo:@Nathan The SP can choose to use the InCommon Discovery Service (but a local, customized discovery service is recommended)
gettes:@nathan that is a capability i am hoping for/expecting from Cirrus
Dedra Chamberlin:Yes, with OAuth providers, SP admins would register with the social IdP, get an OAuth key and secret, and use that to configure the SP in the Gateway manager
Brown - Steve Carmody:june 3, 12 noon EDT
Tom Scavo:@gettes We really don't want to put a discovery service at the gateway, which would put **two** DSs in front of the user
Dedra Chamberlin:Yes, Cirrus is planning to run a custom DS
Dean Woodbeck:Please take a minute and fill out our evaluation: http://www.surveymonkey.com/s/VWG
Dedra Chamberlin:Our plan is to propose a design that will not present a user with double discovery
Steve Olshansky:https://lists.internet2.edu/sympa/subscribe/socialidentity
Steve Olshansky:to subscribe to the list

John Krienke, InCommon/Internet2:I wonder if it would be useful to have a meeting with campus App owners to discuss requirements. Good idea? Or a survey?
Tommy - SMU:i like meetings, but this format for this topic was clumsy
Tommy - SMU:some guys like me just need training/education
Tommy - SMU:others have other conversations
John Krienke, InCommon/Internet2:@ Tommy. Let us know what you'd like to see in the survey. I think we're in the process of developing guidance, but we're not there yet for "recommended practices."
John Krienke, InCommon/Internet2:The working group is definitely where the Sausage is made.
Tommy - SMU:Understood, and I don't intend to be critical - this discussion is exactly what we need more of!
John Krienke, InCommon/Internet2:excellent. Keep the feedback coming.
Tommy - SMU:Slides and discussion were great. Maybe a soup to nuts use case and demo would be the next valuable thing for us as we begin.
John Krienke, InCommon/Internet2:Look for that in fall. And we'll pick up the thread and more at the Identity Week discussion... link ... somewhere ...
John Krienke, InCommon/Internet2:a new meeting – or set of meetings – we're developing with community feedback. http://www.incommon.org/idweek/