Return to Advance CAMP wiki

Advance CAMP Wednesday, Oct. 18, 2017

11:20am-11:10am

Pacific C Room

Authoritative sources for attribute aggregation/External Identities

CONVENER: Niels Van Dijk

MAIN SCRIBE: Karen

ADDITIONAL CONTRIBUTORS: Gail

# of ATTENDEES: 25

DISCUSSION:

Scott: have a version of the attribute for each external source (not delegation -- all asserted by the IdP)
Have a separate named prefixed XML attribute - <saml attribute> original issuer=
Metadata about the attribute
Polymorphic pseudonyms - encrypt and target to a specific consumer. Do the relying parties actually care how trustable the external attributes are?
For the VO scenario, the problem is mostly technical
If the IdP is conveying external attributes, might want to indicate whether IT trusted the attribute source? Or whether it should decorate with student data based on social id authentication?
Scott - We may want to know the inverse - what is the destination of the user? What are they trying to get to? How can we convey this in the authentication event?

Tony Brook - personal notes provided for reference, not complete or actively scribing, for integration with official logs

How to convey source information as part of aggregation.

Proxies - aggregating data from multiple sources.
Institutional IdP - spun up themselves.
ORCID identifier

On other side, push to services, but how does service know what is coming from where.
Another scenario might be dealing with external identities from the perspective of the campus, want to sprinkle attributes - how to do that?

Technically it might be very similar. However, don't know - maybe some other people can do identifiers.

One group doing it with Shib, but doesn't mean standards - they use naming prefix as signalling.

Prefix on the name - one set of attributes are "naked", others are prefixed, and assert or otherwise.

Example - mail, proxiedmail - prefix that comes around. Duplicate the attributes, make sure whole set coming from distinct namespace.

In SAML there is a standard way to use this, but no one uses it. Decorate an attribute.

In collaboration space, Ben can talk for hours, there is the original eppn, then VO creates persistant identifier because provider doesn't allow duplicate.

With original issue / pattern, does it allow duplicates?

Could have 12 with different attributes.

Turns a simple string into an XML that needs to be parsed and interpreted. Shib can do it, nothing else can.

How to show?
<saml:, attribute>
< originalIssuer=>
</>

No capability for transitive trust. Meant to be lightweight. Trust that someone won't decorate. All asserted by a single IdP - not necessarily delegation.

Issue with Proxy.

Microsoft wanted this, big deal. Only time getting to collab on an SAML spec.

Could work for all attributes, because it is metadata about the attribute. It is extensible.

Trusting attributes? Signing? Trust attribute by name. Additional adds get into WSTrust, which should not.

SAML has trust, whereas OIDC doesn't have trust.

Isn't that what OIDC federation is trying, to create trust chains?

Hypothetically you can sign blocks, but no one does.

Basically, proxy would talk to the different attribute authorities. It's just not sticking in signed evidence. If you don't trust your IdP, you have bigger problems.

Even less implemented is Polymorphic pseudonyms. IdP encrypts attribute on the way out, and anything in the way can't read it.

Sounds like a lot of baggage, and that sophisticated.

What seen is Relying parties don't care - they don't care about distinction of origination.
If we end up in future world of long-term identities, isn't it more likely SP will start trusting decorating.

You trust IdP Proxy to give you everything accurately (may be in same domain) - you raise a question if you move it outside. You cannot convince developers to care by policy.

In VO, it is becoming technical. SPs are more tightly controlled (community SPs)

Little worried about scenario where national ID, and institution adds affiliation attributes (eduKEEP) - but then, trust doesn't hold because SP could be Google, or Learning systems.

Two things here - original issuer, apply as separate thing.

Bad thing - gone through a compliance thing - done a certain way, recycle IDs. Then someone thinks it is a good idea to social IDs.

Do you decide how you trust it?

From a campus perspective, external SP may not be playing by the same rules as the IdP, releasing attributes based on their authentication and credentialing, breaking asserting compliance.

As attribute provider, you trust identity provider?

Don't think assurance level is being communicated.

RP want a string they trust.

Service Provider side - they are trusting us to have done the right thing, and middleman.

What would be the issue with asserting affiliation, once it has this kind of thing around it?

If assertion is not coming from us, we don't trust. //

It needs to be done a certain way.

It may not be the topic, but that is the questions.

One of the ways we sell release of directory data is because the user approved. We're not getting in the way.
Standalone queries, there is no way to get around.

Not running a standalone attribute repository for outside consumption.

As software provider, what mechanisms are providing? There isn't a demand for a technical solution.

For types of solutions to take hold,

OIDC model assumes on party aggregation, Hitting APIs independently, rather than have Proxies.
Problem is going to exist in other systems.

Less trust in OIDC versus SAML. OIDC doesn't use public key pairs between entities.

Different tolerance level for crypto.

Use cases are also different.

People forget - This exists because of Google. If it is outside of a use case outside Google wants, question if there is a fit for purpose. Go in with eyes open.

It works a certain way because Google/MS needed it that way. One big IdP.

Best for use case - no one size fits all. Similar JSON tricks for symantecs.

Bigger question is "who cares?"

People don't care much now, but will start to going forward.
Rubber meets the road - cases where social identities fit, and cases where they don't fit (such as students/employees, sensitive data). Where this comes together is in account linking. Want to tie it to institutional ID.

Isn't that already happening? Scenario where you pre-register applicants, where you are asserting applicant.

Institutional credentials vs. Social credentials -
Linking has qualification (to a degree, level of assurance)

In research community, very similar, part of bigger community.

Asked about inverse of topic, what if you want to know what is being accessed on the other end of the proxy. There are ways to express that in SAML. Good behaving proxy shouldn't act as a black box. Externally present endpoints of services.

How do I know destination and factor it in?

Long-term, want institutional credentials?

Will we be releasing that kind of statement against external identities?
Would need a serious legal agreement to not recycle identifiers.

Might mean WE are the ones who care about this, because we care about the solutions. But we want to make differentiation on services, and trust.

People want middleware to solve problem, not write rules.

Root question - trust social ids?

ACTIVITIES GOING FORWARD / NEXT STEPS:

Text here

=====

AggregatedDistributedClaims in OIDC:
http://openid.net/specs/openid-connect-core-1_0.html#AggregatedDistributedClaims
Note: please be sure to link to or attach any key resources from this breakout session