LInk to 2020 ACAMP wiki

Title : ASSURANCE PART 3- WHAT IS THE PURPOSE OF ASSURANCE

Advance CAMP Friday Nov20,2020

11:05-11:55 am ET

Room - Lodge

CONVENER: Andy Morgan

MAIN SCRIBE: Alan Buxey

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES:

DISCUSSION:

Andy - lets kick off with discussion topic that was rattling around near the end of last session Maybe specific to the NIH case.

What's the purpose of assurance? What is NIH gaining from the assertion?

Let's say I used a university process… they know ID is correct, bound to a Gov ID for example… but then IdP has turned around and sent some small set of data… name, (might not be the legal name from the ID proofing doc). Email address - specific to the university… affiliation might be the strongly bound thing…

Pål Axelsson - you as the university are asserting how well you are known as that person (that counts A LOT for some services…)
Christopher Whalen - most SPs aren't going to just accept everything from the IdP - they are going to link that with something else...maybe a PI in the collaboration..something to link with access rights. Quality will be better if providing the extra metadata/attributes of the ID.
Andrew Morgan - ….yeah...as I was thinking about this..the application might be doing their own ID proofing
CW - exactly some of them will be doing EXTENSIVE proofing. Eg they may match the DUNS number to the institution and then link to the grant/PI etc. eg ELIXIR AAI - they have a list of identities to vet against. Going through the process of getting the first credential is pretty expensive (time/manual/etc maybe physical check etc)
CW - I was just looking at a test platform that *UMEA* has? That looked really interesting…
Was looking at attributes being released.. Looks interesting, provides a lot more data.
Pål - will only be available in SWAMID - due to laws etc - checking their own entity category release (R&S, CoCo (a lot of data can be released),
Alan noted the eduGAIN attribute release checker too
Pål - for example we are releasing national ID info… because its needed internally (within Fed) (sequence of 7 tests are being undertaken)
Much easier for a small country than a large country
CW - yes and a federal country like the US is a different thing
Alan - there is a difference between attributes being released and the assurance that those values are correct/up to date
AM - some of the data we're talking about, it might not matter if it's 100% correct….
'Self-asserted values for example, rather than gov ID's
Pål - there is also a difference when dealing with assurance - it's highlighting something else about eg processes...you are showing that you know that person well…
AM - question about unique 1 and unique 2 values in the doc - maybe the SP doesnt know the person well but the IdP does
Pål - in time of need then someone knows that person - can track them.
CW - is anyone releasing ORCID IDs as an attribute?
AW - we did this a year ago..not much takeup if I recall
Maarten Kremers - in surfnet we can inject it - the user has to link it/assert it but its linked as single factor
'Click and connect'

CW - what are we going to have to adjust for uptake - what are the biggest gaps in the assurance framework right now - we talked about mapping relevant guidance internationally to the profile
AM - recently became aware of RAF - a lot of it understandable but I got stuck with how to comply with the high/medium/low requirements . seemed to refer to docs I couldn't find or check. Level x,y,z of some Kantara documentation
Pål - it's not the document now. Kantara have introduced fees to their docs… docs must be open...a hard problem.
AM - if its useful for me to be able to assert then I have to be able to find the documentation. Maybe sections referred to extracted?
MK - sounds like a feasible action to me
CW - i feel there must be a reason why it didn't point to NIST 800-63
Pål - international normalisation
CW - seems strange it wasn't used
Pål - it /was/ - these orgs live on fee etc for access for their service - no Gov funding. (continues) Its better to describe what we are after. When we are talking about this in Sweden we are 'we know this is a person', 'high probability this is the right person', 'indeed checked the documentation'..either directly or via online service at required level. Try to match that against national systems...fed level not university level. So we've done this at national level.
AM - Pål are you able to do this because hub and spoke?
Pål - no, full mesh…. We learnt the mistake of gold/silver/bronze and then adapted to make it less hard.
AM -do you guys decorate additional attributes?
Pål - okay, to make this SAML-ish, we have some type of ...members have to apply for a specific level then we decorate the metadata to show their asserted level. The IdP releases the same values...if they don't then they dont get access to service. ….so, as usual, you need some sort of killer-service , sorry NIH(!)(thats going to be you) NIH will make the required ripple effect in Sweden….even in the Netherlands Maarten!
Maarten - yeh yeh yeh (agrees)
CW - I mean to a certain extent some of this is a ripple effect from GA4-GH (?) , ELIXIR AAI has been here before us… Micheal Linden was one of the ones that lead a lot of this
Albert Wu - so...this might be a tangent...so sorry keep thinking of things towards the edge..'how' we do identity proofing….how does a SP org react to various levels of assurance asserted? With R&S there is a sort of general misnomer that you have to release for all ..thats just not true. Are Orgs misunderstanding/mis-thinking about asking for a certain LoA for Every person in the Org? What does NIH do if LoA DOES NOT MEET the requirements? How does

the interaction between IdP and SP get affected? This detail might make a big change into whether a campus says 'i can do this' or 'there's just no way'
CW- this might make things more difficult
Pål - that might be true?
Janemarie Duh/Ann West (*? sorry, didnt see screen, was just a short q)* really, you think so?
CW - I have 2 or 3 IdPs ...ot as complex as what this community deals with
AW - signalling is trivial….if you haven't done it all though or don't have a business process then this is hard.
CW - we did this with Jeff at UCLA…. For COVID study work…. Some people at the uni medical study faculty - didn't have university credentials...had to deal with that to give them the access
AW - this would be the classic 'guest' users…
AW - a lot of IdPs dont have scalable ways of doing identity proofing because they are so small…. Maybe they end up with very paper-heavy process etc and not much automation
CW - let's look at low-hanging fruit...anyone who is staff...gets a pay cheque/check ...works there - they are in the system.
AW - looking tat those cases might help make campuses make a plan
Pål - agree...but do you think there needs to be guidance?
General consensus - yes...needs to be written down
CW - something needs to be written down, guidance at national level
AM - yes, i think this is necessary….an I9 process or something similar is required. If you can't do an I-9 - if InCommon says 'well you need to look at … (eg driving licence...existing business process' then at least that gives guidance of what you need to do.
AW - yes, this is pretty straightforward ...IAL2, IAL3 and how to map things together for Incommon for th eUS institutions.
MK- i would assume this is true in Europe - have to show ID card to employer … how to link to identity
Pål - that's the hard part..
Maarten - the fact employee exists is implicit
Pål - or that you are paying tax
Alan - at previous employer - HR system knows the person/checks docs etc - that then allows an ID to be created in AD/LDAP….won't appear there otherwise
CW - i have memories of access cards to give only certain access to certain buildings...can be done locally….
MK - what about levels in the Doc - for MFA for service point of view..interop mark, 2-factor needs more quality aspects?
CW - i'm going to turn this around and ask Sandeep

Sandeep Sathyaprasad -
AM - are you talking about the multi factor stuff?
MK - RAF, SFA quite details...but MFA a little blurred...what details?
CW - is there any….i'm sure this exists...but is there something that rates the second factor…. 'TOTP', 'SMS'...etc
MK - yes...SMS exactly...its still allowed in the industry…
CW - but everyone hates it
Pål - one of the problems with MFA is eg Open Fail , discussed earlier this week
AM - maybe not that common...main thing is not to lie about it.
MK - no..but the fact you'd put that into a baseline.
AM - setting this aside a bit..in 800.63 its not that they have these different factors...but as you move up they want specific factors involved….. Is this the distinction you're after?
MK - yeh...that's...well are IdPs able to say its 2 independent factors
CW - i have the same thing for my google ID..sometimes it asks for 2nd factor… and sometimes i'm always being asked . caused me some worry..dont nwo their algorithms
Pål - and that's only a low assurance account..anyway only 1 minute left
AM - do we want to have some actions written down
Pål - CTAB - US how to do things
MK - REFEDS assurance group - take the NIH and see up to what point the spec matches…
PåL - lessons learnt -
MK- yeh, lessons learnt! 'How can we make Chris happy'
CW - how can we make Sandeep happy!
Some general chat/laughter and off record chit chat
CW - I think there needs to be a doc with some international mapping . well help federations that don't have as many resources.
CW - as a final note...just want to thank everyone..you've all been in all these sessions...doing lots of things, have been in many discussions…. Been best week since March..
MK- i agree
PåL - lessons learnt , we've been doing this for 10 years….be good to java outcome
AM (as chair) thanks everyone .
CW - don't hesitate to reach out to us, we're going to organise followup meets.

Meeting ends

ACTION ITEMS: (check against highlighted conversation above)

1. Better guidance in RAF for the low/medium/high requirements
2. CTAB, et al - map identity proofing to national standards, such as I-9
3. RAF - use NIH case and an example to see how the spec satisfies their requirements
4. RAF - link to federation mapping documents