2020 GA4GH Connect Virtual Meeting

Assurance Levels Breakout Agenda

Details subject to change.

Meeting Goals: Determine the advice for the Passports team based on the DSIP on Identity Management

Relevant Work Streams: Security, DURI

Chairs: Francesco Marino & Mikael Linden

Notetaker:

Report Back Slide

March 26, 2020

Start Time	Discussion Topic	Related Materials	Speakers
00:00	Adjusting the DSIP and advice to Passports	slides	Mikael & Francesco
00:00			
00:00			
00:00			
00:00			

Minutes:

Mikael shared slides on assurance levels.
Questions:

- Francesco: What is in the DSIP is too narrow for the scope?
    - Mikael: Want clarity on the NIST spec statement in 3.1.
    - Francesco: The sentence as is may be too restrictive, should be more of a recommendation for the most relevant standards. Should consider including other standards. What are other more suitable standards?
    - Mikael: from the EU approach, I think eIDAS could be mentioned. Not sure about the rest of the world.
    - Kurt: The problem is that several standards are different and may have issues when use in other geographical regions. From the US perspective, some NIST guidelines are mandatory, but can't be made mandatory for europe.
    - Francesco: Our goal of this document is not to make anything mandatory
- Craig: How do we map this into requirements in AAI and Passports as well as other standards. Can be used for implementations to look for certain assurances. The community wants to know if 2 factor auth has been used.
    - Mikael: I think the concrete ways to express assurance follow the open ID connect spec.

    - Tommi: both DACs mentioned that they have a lot of manual work to do to make sure users are who they claim to be. Is there a way to communicate the assurance metadata with the DACs help
    - Craig: I think this is a good tool that could help with this. Should go back to the DACs and see if it helps get more assurance
    - Sarion: IDing the researcher is about “is this a legit researcher with the right to access this data, do they belong to this org” the institutional rep is a different issue. Want to make sure it’s someone with the authority to sign. The delaying part is making sure they are the right signing official. The issue would then be around identifying the researcher.
    - Craig: Does it help reduce risk if you have these kinds of assurance levels including showing you a specific individual did something?
    - Mikael: what does the SO check and how to make his or her burden easier?
    - Sarion: Those things are the right kind of things from the Sanger DAC perspective.
- Marco: (EJPRD): in our federated system we want to process profile matching between the adject requesting access and the data owner. How does this fit together with the DUO and Passport work?
    - Craig: There is lots of overlap with the DUO connector and might help with some of that process. Can help prevent rouge actors.
    - Francis: The critical piece is to provide proportional access based on the purpose of use.
    - Tommi: This assurance is a feature of security, but we need to integrate back to DURI
- Stephanie: When you were thinking about identity validation, could some be alleviated by passports, some of this is part of the broader trust framework.
- Kurt: We cold set up a session to look at all of the alternate ways of working in this problem space.
    - Sarion: Seeing the way the NIH does the institutional representative part of it made me realize there are different ways of doing this.

- Mikael: The ELIXIR AAI ID proofing may be of use here. Slides here.
    - Francis: The passport is hard to have a copy of, so that seems robust, but the photo is trivial to find. One issue is around the sensitivity of the passport photo. How do mwe make this more robust? Inclusion of personal questions: first pet’s name, etc. Create a tech that when the admin gives questions, answers are encrypted.
    - Mikael: The company has proposed a roadmap where this is just the first step.. Next step is to use phone NFC to read the passport. Live video image of passport holder rather than a selfie.
    - Craig: Might not be able to protect against bad actors that are really making an effort to spoof. Fits in multi factor realm.
    - Francis: Check with vendors to see how they are doing identity proofing to find other common standards.
- Sarion: One aspect might be missing. Not just identification and affiliation, does this person still have the right to access this data? Need to give some thought to that too.
    - Francis: The visas in the passports do a good job of that.
    - Mikael: The controlled access grant visa is done within the institutional affiliation context. If they lose that affiliation, they lose access.