https://github.com/ga4gh-duri/Passports/AAI Technical working Subgroup

Security and DURI Work Streams

Minutes and Actions 2022

Minutes for 2021
https://docs.google.com/document/d/1HcvfVTZoS_nz98B5OZBwX_lA4q0ml3wobmIP6Z2YTH8/edit#

Overview

These are the minutes for the Passports/AAI Technical Working subgroup, a collaboration between the Data Security and DURI Work Streams.

This group was formed with the aim of creating a small technical task force to discuss outstanding technical issues regarding v1.0 and migrating to a new version of the GA4GH Passports Standard named v1.2. V1.1 was designated as an experimental release driven within the NIH, known as NIH RAS (details below).

The group aims to produce a summary document and specification to be shared more widely for further feedback and input from various groups across GA4GH including current and future implementers of the GA4GH Passports Standards.

The group consists of AAI and Passports leads, those who have been involved in the development of v1.0 from the start and those newer to the work but with an interest in the technical aspects of both AAI and Passport specifications.

Table of Contents

Overview

Meeting Protocols

Meeting Details:

Specification Build Guide (WIP):

Meeting Minute Report
- 2022-11-17
  - Actions

Minutes
2022-11-10
Actions
Minutes
2022-11-03
Actions
Minutes
2022-10-13
Actions
Minutes
2022-10-06
Actions
Minutes
2022-09-29
Actions
Minutes
2022-09-15
Actions
Minutes
2022-09-08
Actions
Minutes
2022-09-01
Actions
Minutes
2022-08-25
Actions
Minutes
2022-08-18
Actions
Minutes
2022-08-11
Actions
Minutes
2022-08-04
Actions
Minutes
2022-07-28
Actions
2022-07-21
Actions

- Minutes
- 2022-07-14
  - Actions
  - Minutes
- 2022-07-07
  - Actions
- 2022-06-30
  - Actions
  - Minutes
- 2022-06-23
  - Actions
- 2022-06-16
  - Actions
- 2022-06-09
  - Actions
  - Agenda
  - Minutes
- 2022-06-02
  - Actions
  - Agenda
  - Minutes
- 2022-05-26
  - Actions
  - Agenda
  - Minutes
- 2022-05-19
  - Actions
  - Agenda
  - Minutes
- 2022-05-12
- 2022-05-05:
- 2022-04-14:
- 2022-04-07:
- 2022-03-31:
- 2022-03-17:
- 2022-03-10:
- 2022-03-03:
- 2022-02-24:
- 2022-02-17:
- 2022-02-11
- 2022-02-03:

2022-01-27:
2022-01-13:

Meeting Protocols

- Please note that by participating in meetings, attendees agree to adhere to the GA4GH Standards of Professional Conduct.
- Meetings may be recorded for note-taking purposes. Recordings will be deleted within three months of the meeting taking place.
- Dates should be specified in the ISO format yyyy-mm-dd

Meeting Details:

- To join the call please use Zoom
- We will use the Data Security Zoom account

Please use this link:
https://us02web.zoom.us/j/87148565813?pwd=SVVQU3c1SXdIclpQZGRTTDJ6RUhqdz09

GA4GH have added password protection:
Zoom Password = ga4gh
Meeting ID: 871 4856 5813

- Mailing list aai@ga4gh.org

Specification Build Guide (WIP):

Prerequisites (for plain markdown editing)
gh, git

Prerequisites (for local live Jekyll site viewing)
gh, git, docker

```
$ git checkout -b 1.2-draft-DESCRIPTION 1.2-draft-main
$ make
$ browse http://localhost:4000/local/
```

NOTES:
Branches need to be made off the main 1.2 draft and **not** master. The main 1.2 draft branch will accumulate all changes until the spec is finalised - and then the entire branch will be merged over master

`make` can take a fair while - especially on first build - but it then will sit there and do live generation as the Markdown is edited - so this can be done once for an editing session.

When finished

```
$ git commit -a "explanation of changes"
$ git push
```

The resulting branch is automatically published to

https://ga4gh.github.io/data-security/1.2-draft-DESCRIPTION/

The main 1.2 branch lives at

https://ga4gh.github.io/data-security/1.2-draft-main/

Meeting Minute Report

2023-01-26

Attendees (affiliation): Tom Conner (Broad), Kurt Rodarmer (NIH), Michele Mattioni (Velsera), Heidi Sofia (NIH), Larry Holt (NIH), Surja Saha, Marian Cicel (Velsera)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Brief discussion of release being public at https://ga4gh.github.io/data-security/.
Mention of Connect 19-21 April; no concrete plans yet to have any sessions on Passport 1.2.
Michele: It would be good to talk about migration to the new release so users of 1 know a way forward. Perhaps a working session with actual implementors.

2023-01-19

Attendees (affiliation): Fabio Liberante (GA4GH), Tom Conner (Broad), Kurt Rodarmer (NIH), Martin Kuba (ELIXIR CZ)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- GA4GH Comms - Julia Ostmann
    - Tweet review
    - Longer tech & policy blog post
    - Perhaps also check up on Contributor list before announcement
- Launch date?
- DURI Passport needs to link to rendered AAI https://github.com/ga4gh-duri/ga4gh-duri.github.io/blob/master/researcher_ids/ga4gh_passport_v1.md
- Last meeting for Fabio today!
- Steering Committee meeting on 26th January
- Tag release with description https://github.com/ga4gh/data-security/releases

FL: Intro for Julia

JO: Tweet announcement thread - get your eyes on that. Also, a news announcement. Watch for emails. Find the target audience. Guest technical blog post. GA4GH page and where else do you think? Blogs, journals and institutional emails.
FL: Twitter handles for contributors?
KR: Not digital identity.
Rephrased.

TC: Will add Passports link to DURI rendered GitHub. And fix TOC issue in spec itself.

TC: Release creation.
MK: Tag and then release.
MB: AAIv1.2 copy style. I will push a tag.

Release created.

Repo description and website link updated.

MK: EGA? Life Science RI. GHGA. Both consume Visas from Life Science RI.
KR: Mike Feolo - best person to contact about NIH RAS “paperwork” side.
feolo@ncbi.nlm.nih.gov

Send twitter to the rendered profile. All +1

TC: Link back to GitHub from the rendered version?
MB: For the future.

Clarify “Cloud IAM/AAI” scope. Is this ELIXIR only?

MB: What do we feel about weekly 1 hour meeting now 1.2 is out? Ideation phase for 2.0.
MB: Monthly? Or regular AAI WS meeting?
TC: +1
MK: +1
KR: +1

2023-01-17

Extraordinary meeting - 1.2-draft-main merged with master branch. Minor corrections from here.
Jekyll render worked beautifully. Release to be tagged on Thursday.

2023-01-12

Attendees (affiliation): Fabio Liberante (GA4GH), Max Barkley (DNAstack), Kurt Rodarmer (NIH), Andrew Patterson (UMCCR), Tom Conner (Broad)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- Reviews - all issues addressed or acknowledged
- Implementations
    - Martin Kuba - Life Science AAI now implementing v1.2
    - here is documentation how to get an account in LifeScience AAI: https://lifescience-ri.eu/ls-login/users/how-to-get-and-use-life-science-id.html
    - demo service using Passport 1.2: https://echo.aai.elixir-czech.org/
- Launch date - merge branch today and “launch” 19th January?
    - ~~Steps to launch~~
    - ~~Settle on diagrams~~
    - Known limitations section
    - Check/tidy FAQ and Changes sections
    - Passports Repo URL links - cross reference
        - Need to update AAI to rendered DURI - TC to do
        - DURI Passport needs to link to rendered AAI https://github.com/ga4gh-duri/ga4gh-duri.github.io/blob/master/researcher_ids/ga4gh_passport_v1.md
    - Remaining meetings for Fabio - 19th January NEXT WEEK
    - Steering Committee meeting on 26th January
    - GA4GH Comms Team waiting to announce

- Update README to link to rendered Jekyll page e.g. https://ga4gh.github.io/data-security/1.2-draft-main/aai-openid-connect-profile and perhaps a version list
- Fabio can follow up with GA4GH Comms. May need help articulating the Passports/AAI interplay.
- Tag release with description - FL will write - authors & reviewers
- https://github.com/ga4gh/data-security/releases
- Check contributors!

AP: GitHub action will wipe 1.2 rendered drafts. Commit history will remain.
AP:

MB: A sentence for why we introduce a token exchange mechanism. It will be scoped in future.
KR: Audience would break a current use case. Can't use the same token between nodes. Seven Bridges to dbGaP would be broken. There are other mechanisms we can work towards. Work Order Token. Max?
MB: We haven't mentioned audience. We have to say that it will be addressed in a future version.
AP: Scope not really audience, but that's what I'm trying to get to. This is

AP: We need to address why we add Token Exchange? I take Kurt's point.
AP: Nuke Known Limitations section.
KR: +1
MB: Ok with fixing it and **removing it**.

Client Software - section
KR: Who has implemented this?
AP: Me.
KR:
MB: PKCE is on mobile apps, security for OAuth login hijacking. A rogue app can redirect with a code and get the access. Integrity of login flow. Change first sentence in FAQ.
AP: frontend React scenario and mobile flow. On a mobile phone that can be hijacked. Solved by PKCE. Deprecated the other flow, Implicit.
MB: Implicit flow has been deprecated for mobile and SPA.
KR: Where does the token live after being given out?
MB: If a SPA it gets the token at the end of the flow.
AP: In the Javascript store in the browser. The issue is I'm not sure how it can do a Token Exchange correctly from that point.
KR: We have requirements about handling tokens. We can't persist them in plaintext and vulnerable to leakage.
AP: This the same as secure cookies. Browser is securely storing cookies.
KR: Except when browser isn't a browser. Different protocol for SPA. Forcing them to use brick and mortar server that retains the Tokens that they establish.
AP: That's what we are proposing.

KR: Suggest it is given as one possible way of doing things. Different protocol to keep all tokens away from the browser.
AP: We didn't end up using PKCE ourselves. SPA just triggered that flow.
KR: Sounds like an approved way.
TC: Tone is too gentle. DON'T STORE TOKENS WITH PKCE.

AP: **I will take this.**

Changes section –
MB: +1 for everything in there. **What about changes from reviews?**

FL: **Check in with MK about DURI Passport links.**
FL: **Readme - send to TC**
FL: Author list - send around

AP: TC & MB as admins.

FIND A TIME FOR NEXT WEEK TO MERGE PR ALL TOGETHER.

2023-01-05

Attendees (affiliation): Tom Conner, Kurt Rodarmer (NIH), Christopher Siwy (NIH), Larry Holt (NIH)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- Reviews - all issues addressed or acknowledged
- Implementations
    - Martin Kuba - Life Science AAI now implementing v1.2
    - here is documentation how to get an account in LifeScience AAI: https://lifescience-ri.eu/ls-login/users/how-to-get-and-use-life-science-id.html
    - demo service using Passport 1.2: https://echo.aai.elixir-czech.org/
    -
- Launch date - 19th January?
    - Steps to launch
    - Settle on diagrams
    - Check/tidy FAQ and Changes sections
    - Passports Repo URL links - cross reference
        - https://ga4gh.github.io/data-security/check-links/
    - Remaining meetings for Fabio - 12th & 19th January.
    - Steering Committee meeting on 26th January - would be a natural deadline to aim for.
    - Fabio can follow up with GA4GH Comms. May need help articulating the Passports/AAU interplay.
    - Tag release!
-

TC: ~18 links from DURI to AAI. A couple older anchor links broken, added extra anchors to AAI side. Replace base URLs.
TC: Do PR directly to update this in DURI repo. Will check with Martin if not possible.
TC: Avoided wordsmithing the Passports spec for now. Keep links the same.

Rendered Passports here https://ga4gh-duri.github.io/researcher_ids/ga4gh_passport_v1.html
Seems to be autorendered on commit.
TC: Caught broken links in AAI spec.

TC:
https://ga4gh.github.io/data-security/check-links/aai-openid-connect-profile#flow-of-assertions
Diagrams.
FL: Any issues/problems with flow of assertions?
MK: ELIXIR is something in between two given examples. Happy with this.
KR: +1

https://ga4gh.github.io/data-security/check-links/aai-openid-connect-profile#conformance-for-passport-issuers
FL: Any issues?
MK: Visa Issuers - multiple issuers for one DAC? Reason?
TC: None. I'll make single issuer for each DAC in same PR.
CS: Visa B & Visa C obtain. Is that to show you can have one or multiple to come from an Issuer?
TC: Yes.
CS: +1

KR: In FAQ diagram - RS256 listed, when we recommend ES256?
MK: Generic <alg-id>
TC: Will do.

MK: Expiry is listed as 60, which is 60 seconds. Not realistic.
KR: This is only an access token.
MK: This is the response, no?
KR: It is.
MK: Does expiry need to be there?
ACTION - ask Max!
MK: RFC lifetime in seconds recommended, but not required. Could drop it?
KR: Expires in update. Purpose is to echo the duration of the token being returned. So the receiver does not have to decode the token, but it is redundant information. I recommend we drop it from the diagram. Passport speaks for itself.
MK: In spec, the token may be opaque. Still drop it.
TC: Just pushed - add Max as reviewer.

FL: **Missing question mark** in FAQ "What is the danger of using a fully scoped (or audience-less) token in a multi-node workflow"

KR: I have argued against this before. "Threat analysis in FAQ" - something to be handled by WOT. The idea for the audience is using Passport as WOT.
TC: Do we keep it?

KR: This is an argument for complete OAuth flow - which we don't have.
KR: Downscoping requires intermediate authority, which starts to get really gnarly.

FL: Change Threat Analysis title?
MK: +1 Just delete it.

MK: Drop "The safer alternative is a system where passports can be down-scoped before use - the Passport that is maliciously being passed from Resource Server #A to Resource Server #B would then be rejected - because it would be scoped only for Resource Server #A / Dataset #1." & "The addition of audiences to the token, or down-scoping of permissions - possible via token exchange - limits the scope of damage if the token ends up with a bad actor." from this section.
TC: +1
KR: Known limitations then?
KR: "Known limitations of audience scoping"

Follow up discussion on this section

2022-12-22

Attendees (affiliation): Martin Kuba, Tom Conner, Christopher Siwy (NIH), Larry Holt (NIH), Heidi Sofia (NIH), Kurt Rodarmer (NIH)

Apologies:

Actions

Actions Arising	Assigned To	Deadline
Push PR for changes discussed during meeting	Tom	22 Dec
Check URLs	Tom	

Minutes

Discussed diagram changes and Visa Assertion Source definition change.

2022-12-15

Attendees (affiliation): Max Barkley (DNAstack)l, Tom Conner

Apologies:

Actions

Actions Arising	Assigned To	Deadline
Visa Assertion Storage		
Check URLs		

Minutes

Agenda

- Reviews
    - Francis Jeanson (remaining edits) - FJ - 1.2 Draft Main Branch on 20221013
    - Timothy Slade - RB - 1.2 Draft Main Branch on 20221013
    - https://ga4gh.github.io/data-security/review-2022-12-01/
- Implementations
    - Martin Kuba
- Launch date?
    - Steps to launch
    - Passports URL links - cross reference
    - Remaining meetings for Fabio - ~~15th Dec,~~ 5th, 12th, 19th January.
    - Steering Committee meeting on 26th January - would be a nice time to aim for launch.

FJ review - double checked. Only notable changes/motivations bullet still needs added. DONE - in PR.
RB reviews - double checked. **Visa Assertion storage** comment? - TC will draft something. MB - Easier by changing the order of Visa Issuer and Assertion Source definitions? Will make comment in PR to discuss Asynchronously.

TC: Will **check URL** at both sides between DURI Passports & Data Security AAI. <To tag Martin on any changes to DURI repo>

2022-12-08

Attendees (affiliation): Kurt Rodarmer (NIH), Fabio Liberante (GA4GH), Heidi Sofia (NIH), Tom Conner (Broad Institute),

Apologies: Martin Kuba,

Actions

Actions Arising	Assigned To	Deadline
Simplify flow of assertions diagram per discussion	Tom	
Convert passport conformance diagram to sequence diagram	tom	
Nix Google Authentication	tom	
Check with Timothy on Revocation	Fabio	

Minutes

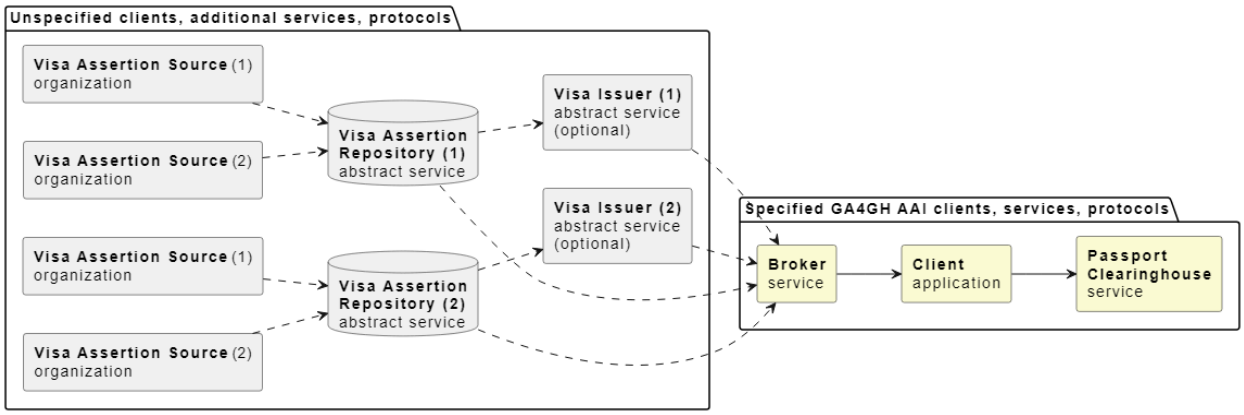
Agenda

- Reviews
    - Francis Jeanson (remaining edits) - FJ - 1.2 Draft Main Branch on 20221013
    - Timothy Slade - RB - 1.2 Draft Main Branch on 20221013
- Implementations
    - Martin Kuba
- Launch date?
    - Steps to launch
    - Passports URL links - cross reference
    - Remaining meetings for Fabio - 15th Dec, 5th, 12th, 19th January.
    - Steering Committee are meeting on 26th Janaury - would be a nice time to aim for launch.

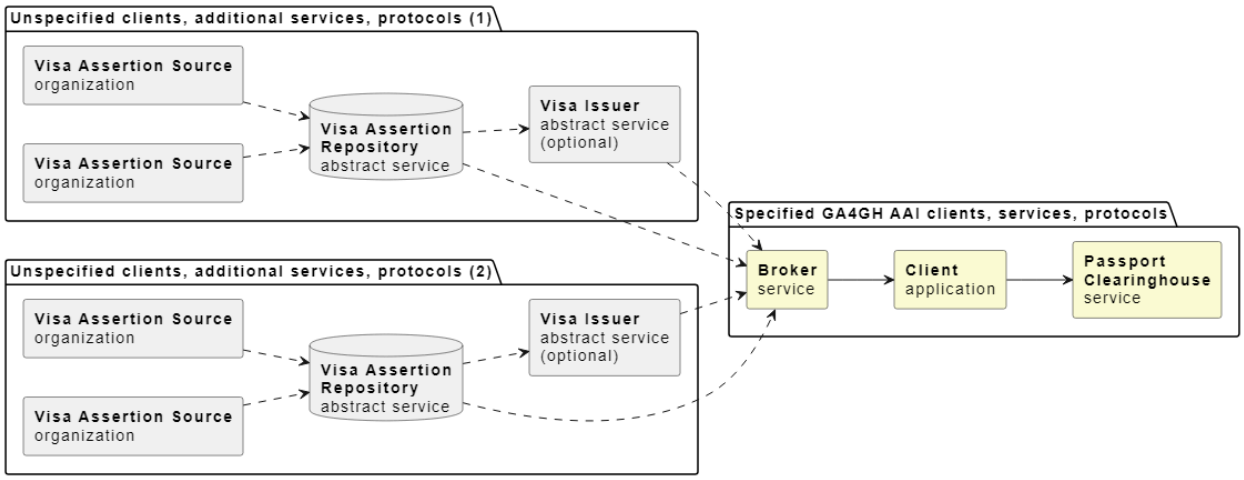
TC:
RB review - points covered in PR, except diagram finalization.
https://ga4gh.github.io/data-security/review-2022-12-01/aai-openid-connect-profile
https://github.com/ga4gh/data-security/pull/94/files?short_path=7c170ce#diff-7c170ce184e7c251204b8cab8667ef4593c9dede7ad27b19c4e185c612f11627
Reflow Markdown? Dramatic diff, but cleaner source.

Flow of Assertions diagram. Multiple sources and repositories for Visas. A or B option?
Emphasize differences between organisations?

A–

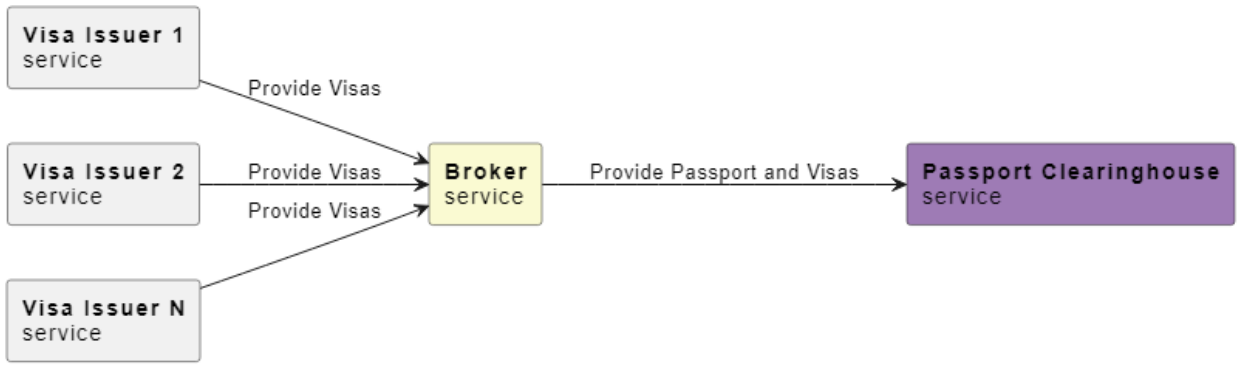


B–



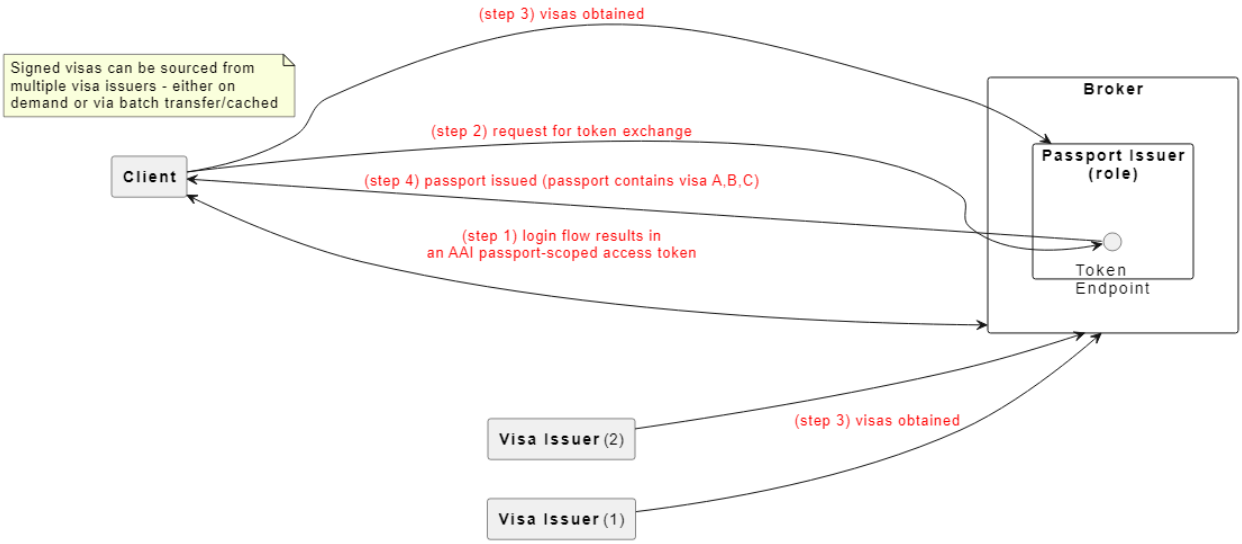
KR: This illustrates one concept, not all. It doesn't clarify Visa Assertions. Makes its seem world is full of VIsa issuers and aggregated by a small number of Brokers.
TC: I agree. Wrong idea.
KR: Visa Issuer and Broker do not need to be separate entities. Different Roles. Clearinghouse and Visa Issuer should not be in the same box as the Client. Not part of this, clients of this.
TC: simple one to relationship.
KR: Simple diagram is a disservice. Two diagrams also confuses this. And neither represents a general case. What do we do now?
TC: **Simplify it back** to the FAQ version. Flow of Assertions with no repositories.
KR: Multiplicity in the lines? Multiplicity at both ends. Many to many Visa-Broker relationships.
TC: N&M on ends of the arrows?
KR: Textual that this can play out in several ways. One-to-one at NIH, but general model is many-to-many. ELIXIR is many-to-one. Important that you don't get the multiple Client situation from the diagram. Pitfall of this entire effort, we don't understand or give importance to both ends of the flow. Broker and AuthZ/N importance, but not the Clearinghouse.
TC: Like your idea of collapsing it down. We would pick one or the other. Simpler.
KR: Assertion Repository is a throwback to the original design. Universities would centralize on a resource, like the ELIXIR model. NIH is not this model.
TC: Adds confusion. No more boxes.
KR: If we want to discuss other cases, we can.

KR: Google Authentication - can we nix that?
TC: +1



TC: Many to many indicators of multiplicity. But it doesn't have the application.
KR: Could be amorphous. What's in between is less clear. Endpoints that are being specified.
TC: I will have a go at a radically simplified diagram.
KR: Opportunity to illustrate. Clearinghouse has to understand the visa - only.

TC: Helpful to engage with Creative teams in future.
TC: Define roles. Terminology in words. Diagram flow visually. Person with authority to the application doing the work.



Yellow note jumped - lower right between Issuer and Broker.

KR: Same thing as what we were talking about, but different enough to confuse. We have not created a birds eye view of major components and then zooming in on the minor components. This diagram is about getting your token.
TC: Birds eye view is the previous one? This diagram is very close to log in and token exchange and interaction. OAuth conventions - sequence diagrams are an organized way to show this.
KR: +1

TC: If it deserves a diagram, it should be **a sequence diagram**.
KR: This solves the bird's eye view.

TC: Make an edit to the PR - to back away from this diagram.

TC: FJ review may need reread later.

TC: Need clarification from Timothy whether revocation is now clearer.

2022-12-01

Attendees (affiliation): Tom Conner, Kurt Rodarmer (NIH), Christopher Siwy (NIH), Heidi Sofia (NIH), Max Barkley (DNAstack), Martin Kuba (ELIXIR-CZ)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- Reviews
    - Francis Jeanson (remaining edits) - FJ - 1.2 Draft Main Branch on 20221013
    - Timothy Slade - RB - 1.2 Draft Main Branch on 20221013
- Implementations
    - Starter Kit?
    - Release Candidate concept
- Launch date?
    - Steps to launch

Timothy Slade review

RB - 1.2 Draft Main Branch on 20221013

No internet connection needed for signatures - “signatures 101” pointers in FAQ?

“The recommended approach” is unusual for a specification. Replaced in branch.
“Stores the assertion” - this is an abstract concept outside the specification.
In ELIXIR multiple Assertion Sources and Repositories and Visas created from all of them.
Create this in an amended diagram. Remove optional from diagram.
NIH RAS team - want to understand why we will deprecate the Visa Access Token instead of the Visa Document Token. KR: Moving toward embedded Visas with v1.2.
MK: It was never used in any implementation and complicates things. Visa must be created specially and can be leaked as an access token.
MK: No one is using it and you don’t want the Visa to be an access token.

Token Exchange diagram - agree that changes need to be made. Bidirectional arrows for login flow and move Visa Issuer note alongside.

Access token validation needs tidied up.

2022-11-24

Attendees (affiliation): Fabio Liberante (GA4GH), Martin Kuba (ELIXIR)

Apologies: Thanksgiving!

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- Reviews
- Implementations
    - Can we link out to ELIXIR prototype as example usage? Or is this risky?
- Launch date?

MK: Will try to make time to provide feedback on RB & FJ reviews. Will also follow up on the situation with Life Science AAI v1.2 implementation. New platform relies on GEANT and ELIXIR systems together. ELIXIR are ready to deploy, GEANT not yet.
FL: Can we make a “fake user” demo system?
MK: This is contrary to the purpose of AAI, so won’t tell us (or implementers) much.

2022-11-17

Attendees (affiliation): Fabio Liberante (GA4GH),Tom Conner,,Kurt Rodarmer(NIH), Max Barkley (DNAstack), Bruce Hoff (Sage Bionetworks)

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- PPIDs in Passports. How should we acknowledge this issue?
- Reviews
    - Francis Jeanson review complete - FJ - 1.2 Draft Main Branch on 20221013
    - Timothy Slade review complete - RB - 1.2 Draft Main Branch on 20221013

KR: Access control and authorization are completely separate systems. DAC vs resource provider.

FJ - 1.2 Draft Main Branch on 20221013
MB: Like suggestions to talk about why changes were made.
TC: 3 covered elsewhere - 2 take or leave.
MB: Question about what to do with token. Good to explain why we didn't want to share that token, but we could pull text from elsewhere.
FJ - 1.2 Draft Main Branch on 20221013
MB: While not normative, it helps understanding. Maybe make clearer the non-normative parts?
TC: Visa Assertion is specified, but topology is not.
MB: Emphasize network topology is not defined?
TC: VAS and VI are normative, VAR is not. Go back to the older diagram? Simpler flow. The exception is many to one and cached situations.
MB: VAR is only non-normative part.
TC: VAR mentioned as a possibility instead?
MB: Maybe we could
KR: Outside the box?
TC: Just remove the boxes?
KR: I find the boxes bothersome.
MB: A) We get rid of boxes and VAR and change our sentences. The services are defined, but not the protocols.

TC: Could put the VAR in FAQ?
MB: Ambivalent. Not an FAQ.
TC: Just simplify diagram.

Timothy Slade RB - 1.2 Draft Main Branch on 20221013
KR: Do we have an example token?
MB: I don't think so?
TC: DURI spec?
KR: Could question, DURI spec?
MB: I have not reviewed the DURI spec. Only the PRs Martin sent.
KR: From the beginning claims formed from DURI side, web communities are fond of URLs. What I presented with WOT, in part because I didn't use those ways of expressing things.
TC: We need to unify the Passport/AAI spec into one after v1.2. Truth is currently spread across two different documents.
MB: Happy to do a review of the Passports spec.
KR: Visa embedded in a Passport can be validated without network connectivity. Other options do.
MB: Important aspect of wanting to validate offline.
KR: Will Visas be inside Passport?
MB: Yes.
KR: For cases where the Clearinghouse cannot access the network.
TC: Validate offline if you have the public key.
KR: Red herring to focus on signatures. Clearinghouse validates more than just signatures.
TC: Embedding Visas inside Passports is the trick.
MM: I don't understand the content? The Visa signature is what you validate.
KR: Does anyone assert that v1.2 Passport allows the Visas not to be included in the Passport?
MB: Passport-scoped access token, Passport itself always have Visas.
KR: Carrying over an old argument that's no longer relevant. In v1.0 - Passport does not contain Visas. Main difference is whether you retrieve them or include them. We don't need to go over this again.

RB - 1.2 Draft Main Branch on 20221013
This is nice idea, but a lot of work and not necessary.

KR: Is there any mechanism for addedums after specification is released?
MB: No current small release, but good point.

MB: dbGaP custom visa asserts a lot of things about a user, but this is getting into the weeds. Typically 1:1, but it is possible to put multiple assertions in a single Visa.
TC: Visa Assertion is not about a user?
MB: The assertion for controlled access is granted to a user.

BH: I would like to ask a basic question (with apologizes for lacking background knowledge for this standards group): What is the *standards development process* that GA4GH requires this group to follow, what are the required steps and artifacts created along the way, and where may one find these artifacts? In particular where are the use cases that allow one to ask whether each element of the standard is both necessary and sufficient? I didn't immediately see the answer here, https://www.ga4gh.org/how-we-work/ or here, https://www.ga4gh.org/how-we-work/strategic-roadmap/ so I thought I'd ask in this meeting. An example process from "Open Standards for Data" https://standards.theodi.org/creating-open-standards/developing-standards/scoping-and-starting/
has the element:
"The scope, features and use cases: that demonstrate a strong reason for creating the standard, compelling scenarios for how the standard will be used and the core features it will contain"

2022-11-10

Attendees (affiliation): Martin Kuba, Tom Conner, Heidi Sofia (NIH),

Apologies:

Actions

Actions Arising	Assigned To	Deadline

Minutes

Agenda

- PPIDs in Passports. How should we acknowledge this issue?
- Reviews - Francis Jeanson has begun reviewing here.
- Preparation needed for Workshop next week?

MK: Let's mention that PPID may be used, and that the sub of Passport may need to be correlated to the subs from visas using LinkedIdentities visa. action - Martin will add it to the spec (done: https://github.com/ga4gh/data-security/pull/90/files)
Francis Jeanson's comment were considered one by one, some accepted, some not.

2022-11-03

Attendees (affiliation): Martin Kuba, Fabio Liberante (GA4GH), Max Barkley (DNAstack), Marian Cicel

Apologies: Kurt Rodarmer, Andrew Patterson, Tom Conner

Actions

Actions Arising	Assigned To	Deadline

Minutes

Bruce Hoff Comment on Spec
https://docs.google.com/document/d/19TNnieQuVYbFD9po3H8fXlFNDuC1DnrVABA0ybVgXl0/edit?disco=AAAAi7HNJPc
Is there any authentication in this request besides the passport? If not, how does the "Clearinghouse" know which of its registered users is making the request?

OIDC spec says SHOULD using pseudonymous identifiers in “sub”.
MB:
MK: ELIXIR is sending ELIXIR ID - unique ID for all services. Facebook is the only provider I know doing this (PPIDs). GitHub, ORCID, Google etc. all use the same user ID for every client.
MB: DNAstack - not using PPIDs either.
MK: Fix this by saying that sub should be the same for all. Need to correlate between services.
MB & MK: will add to spec that PPIDs must not be used by Passport, sub MUST be the same between. <public> see https://openid.net/specs/openid-connect-core-1_0.html#Correlation:~:text=by%20this%20specification%3A-,public,-This%20provides%20the

MK: Spec currently defines sub in Passport Scoped Access Token and the Passport itself.
MK: Need to think about this longer. There is no way to get other information about the user - as UserInfo isn’t contacted.
MB: Depends on the goal. If you need a user’s name and email - that can’t be fixed right now. If you need a unique ID - only the original client would be able to do this.
MK: Clearinghouse allows access based on the Passport contents. How this is done is out of scope. ELIXIR is by subject. Maybe we don’t need to specify at all.
MB: The assumption is that the Data Holder looks at the Visas to decide if they release data. What are the requirements that the Data Holder would have to know the user?
MK: Add comment to inspect Passport itself and not the user.
MB: Using this between organisations - need to track malfeasance.
MK: With passport - you cannot actually.
MB: Broker and Issuer are different - the Clearinghouse would need to follow up in a separate channel.

[Minutes interrupted - see Recording until updated - NEED to circulate question/discussion on this]

Problems

- How does a clearinghouse contact a user (i.e. get their name and email address) if there is malfeasance?
- Is it a problem that the same user may have different subject IDs in their passports from different clients?

Options for subject in passport:

- Allow pairwise/PPIDs (passport might need to contain information on which client obtained that passport for broker/issuer to identify user correctly)
- Only allow public IDs (i.e. no pairwise/PPIDs) so users can be correlated

Options for clearinghouse to identify user

- Don’t provide any way of doing this in the spec; must be done out-of-band

- Recommend that clearinghouse requires additional token with user information if they require it

Reviewers

Connect Session Preparation
—

2022-10-13

Attendees (affiliation): Tom Conner, Max Barkley (DNAstack), Martin Kuba, Marian Cicel (SBG), Fabio Liberante,

Apologies: Kurt Rodarmer, Andrew Patterson,

Actions

Actions Arising	Assigned To	Deadline
Diagram change	MB	
Add links	TC	
Google Doc for review	TC	
Send for review	FL	

Minutes

https://ga4gh.github.io/data-security/1.2-draft-dg-intro-feedback/aai-openid-connect-profile

FL: Larry Holt as 3rd reviewer on hold. (Agreed).

MB: <Going through PR #88>
Moved Background into FAQ
Add Client section to Technical Summary (Agreed)
#Client broken link to fix
Overview of Interactions super heading over Flow of Assertions - and moved down. Stripped FAQ diagram.
MK: Arrow between Visa & Passport Issuer?
MB: Removed those as non-normative and not part of the spec.
MK: Spec specifies that Broker collects the Visas
MB: Spec clarifies that the mechanism for obtaining Visas is non-normative, Visas are.
MB: Do we add a note somewhere? I like that few of the arrows are not specification.
MK: Sequence diagram shows actions that should happen. This action is missing. Before response with Passport.
MB: Add back informative only section?
MK: Broker can also be Visa Issuer.
MB: RAS just looks into dbGaP.
MK: Broker must always get the Visa somewhere.
TC: I think it adds clarity. Regular arrows.
MB: Between req and response of Passport.
TC: Not a valid sequence diagram without a call/response for Visas. Only an example flow.
MK: Not sure how you would suggest
MB: Exchange of Visas double arrow (protocol unspecified)?
+1 from group.
+1 for surrounding text.

MC: Back to the diagram. Exchange of Visas - sequence is important, it may happen before the client/response. Maybe it's an optional step. Can happen asynchronously.
MK: First you need to identify the users. Usually get fresh Visas at that point. Unless refresh from Cache.
MC: Optional step?
TC: If needed captures it?
MK: Still put it after the request for Passport.
TC: Strike protocol unspecified - as less wordy.
MB: I feel it should stay.
MC: Protocol specified?
MK: ELIXIR did specify in their implementation.

MK: Endpoints VIsa Issuers should have?
MB: Implies JWS endpoint.
MK: Just one?
MB: I think so.
MK: It was surprising, but it's fine.

TC: Make defined terms be links (I can PR) & RFC.

MB: Intro links tidied up.

MK: Intro second paragraph is maybe outdated? Claims is old terminology. What the word be?
MB: Remove claims and just link to researcher authorizations and attributes.
MK: Claim had two meanings - Assertion and JSON spec.

TC: Passports link should be added to Bibliography as an external link. I will do it.
MB: I will push my changes first.

MK: Clearinghouses without Passport?
MB: I can fix that. Pushing.

TC: I will add links to Intro.

TC: Pushing my changes and you can refresh.

MK: OIDC between GA4GH and AAI and self link.
TC: I will tackle that.

MB: That's it for the review?
MB: Approval from Andrew.
MB: Merge?
+1
TC: Google Docs - FL to send to Larry Holt.

Sync by email - meeting on hold until Larry has reviewed the latest draft.

2022-10-06

Attendees (affiliation): Tom Conner (Broad), Christopher Siwy (NIH), Kurt Rodarmer (NIH), Heidi Sofia (NIH), Vivian Ota-Wang (NIH)

Actions

Actions Arising	Assigned To	Deadline
Check for Broker NOT Passport Issuer Use case		

Minutes

TC: Went through everything that was easy. I did not touch the more structural changes. Conformance sections etc. Propose walking through the changes so far in PR 87
https://github.com/ga4gh/data-security/pull/87/
Then we tackle bigger issues in a second run through.
MB: +1 for this approach
TC: IEEE square brackets set apart links to external specs.
TC: Do we alphabetize or separate inherited definitions?
KR: I will make some edits to this PR.
MK/MB/KR: Square links and alphabetize +1
TC: Hand over to MB for bigger questions in original Google doc review.

MB: Discuss flow of assertions section. RFC would have a contextual diagram. Instead we only show assertions to broker. Not suited to be first before a more general diagram. Broker/Visa Issuer/Clearinghouse etc.
KR: +1 - We don't have any reference to where the assertions come from.
TC: Talk of inlining the intro? That has a different diagram.
VOW: Detail is good. As much as possible. Not sufficient for processes we need here - can be a source of anxiety.
HS: Good point, but we need a crisp spec with a target audience in mind.
VOW: A snapshot of the process. People just cutting and pasting - without realizing it's a floor not a ceiling.
MB: Do we need a more detailed example - like the FAQ? My feeling Intro & diagrams. Maybe less detail. Cut out all non-normative parts.
TC: The FAQ diagram would be stronger by removing the bulk as you said.
MB: Will create PR for Intro/FAQ.
CS (in chat): I agree, I think the sequence diagrams of the flows are helpful in presenting the visual overview (as Max alluded to), and helps communicate two audience needs (those that

would like to present the visual, and those that would like to dig into detailed explanation in the text).

MB: Visa Access & Document Tokens are two very different and significant architectural decisions. Maybe hoist to top level of different paths. Second heading?
TC: Highlighted Deprecation warning was in a later version. That plus re-ordering Document & Access order should be enough.
MK: Could just link to Access Token in the older version of spec and remove entirely?
TC & MB & KR: +1
MB: DG viewed an Issuer as a Broker - essence of Broker is not defined. Broker aggregates Visas.

MB: Confused about which things are “defined” for Document Token.
MK: In ELIXIR we define permissions API - interaction of Visa Issuers. Entities for
KR: In our system there is no separate means to get Visas at NIH except Broker.
MK: A sentence about what is NOT defined rather than what is (e.g. Broker-Visa Issuer interaction)

KR: Any Broker needs to back up what they are delivering with a token. I’m not sure what a Passport Issuer that is not a Broker looks like.

TC: Fix symmetry with second diagram.

MB: DG Q - where is the Passport Clearinghouse? A Clearinghouse doesn’t need to be connected to a Broker, but it is in the diagrams. Clearinghouse is only shown in an attempt to access data, so roles are clear.
TC: +1
KR: Right to left arrows - is there a reason? English text/diagrams are usually L-R.
TC: See live version.
MB: Leave it.

MB: Add client between Broker and Clearinghouse in FOA diagram.
TC: I can create a PR.

MB: Clients aren’t listed in the Intro. Maybe insert that Clients are a separate party?
MK: +1

MB: Confusion between Clearinghouse and a Visa Issuer.

MB: “issued by Broker” is removed from title.

MB: DG Q - Duplication between Visa section and the conformance section.

Some options to consider:
1. We move all the token format sections to be sub-sections under the "Conformance of X" sections, respectively
2. We try and remove the requirements of what's in the token from the Visa section, link to this section from above
3. Go with the original suggestion of moving this section to the "Conformance for Visas Issuers", leaving the others alone
MK: I was also confused by why the same thing is defined in two places. +1 for 1.
TC: +1 for 1. I will do that.

TC: Sharing again. Client in the middle diagram.
KR: Mostly white with dark purple.
MK:
VOW: Some people can't see color. Patterns or dots instead?
KR: Both?
KR: If we start with a token as origin - data access to the right?
MK: remove AAI spec over the arrow.
MB: What do we want to convey by colours? Luminance instead.
TC: Client isn't defined in this spec.
MK: Inherits OAuth defs.
TC: (unspecified) arrows?
MK: The interactions are not defined.
CS (in chat): Dashed for unspecified

FL: Connect "release workshop" potentially?
MK & MB: Avoid further open reviews.
MK: We could create a patch version from that feedback.
CS (in chat): Good idea @Christopher

2022-09-29

David Glazer and Dylan Spalding have completed their reviews of the draft AAI v1.2 specification. The Google documents are here (DG) and here (DS). They are open for commenting - so please comment directly if you have a response or suggestion.

Attendees (affiliation): Tom Conner (Broad), Martin Kuba (ELIXIR CZ),

Actions

Actions Arising	Assigned To	Deadline

Minutes

DS REVIEW -

MK: Could remove Data Controller entirely? Delete the definition. Only times it's referenced is in Data Holder - could change those to DAC.
MB: Summarizes.+1
TC: +1
TC: Will start PR.

MB: Not require refresh tokens, as it adds to req beyond OAuth2

TC: Maybe replace Revoking Access Tokens from Bad Actors section entirely?
MK: I would remove it to make specification shorter and more easily understandable.
MB: Slightly in favor of removing this section. Best practices
TC: Limited damage of leaked tokens similar.
RFC6819 - Lodderstedt, T, McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", RFC 6819, January 2013.
RFC8725 - Sheffer, Y., Hardt, D., and M. Jones, "JSON Web Token Best Current Practices", BCP 225, RFC 8725, DOI 10.17487/RFC8725, February 2020.

MB: +1
MK: +1

General issue with Capitalization of SHOULD/MUST.

MB: Remove refresh token rotation from Conformance for Visa Issuers section

MK/MB/TC: Remove the entire Token Revocation section.

DG REVIEW -
TC: No changes needed to the main spec for things already in the Introduction section.

MK: Most definitions are inherited, e.g. Flow from OAuth2 and OIDC.

TC: Call out Passports more explicitly. This spec and that spec - matched pair. Old version didn't use Passports at all.

MB: Emphasise an external specification. Passports.
TC & MK: Reference to Passports terminology. And one sentence to explain.

VOW: Assumption of naivety is an important one. Should consider running it past someone afresh.

MB: Maybe inlining the Introduction would actually be the best option here. Now that it's shorter. Replace Abstract with Intro?

TC:
MB: External terms section

VOW: People do invoke documents. Being explicit helps.
MK: Confusing a claim as a key and value in the technical sense.
TC: The definition is unclear anyway.
VOW: Claim is interpreted as a legal term.
MK: I made sure that the word claim is only ever used in a technical sense.
TC: Agree with VOW.
VOW: Nuance that is important.
MB: Positive not negative language.

2022-09-15

Attendees (affiliation): Tom Conner (Broad), Andrew Patterson (UMCCR/BioCommons), Christopher Siwy (NIH), Heidi Sofia (NIH), Vivian Ota-Wang (NIH)

Actions

Actions Arising	Assigned To	Deadline

Minutes

Reviewers.
FL: Still prodding reviewers for response. Nothing back yet.

Discussion around implementation.
AP: Have some code based on a NodeJS implementation, but there were issues in the peculiar way the OIDC flow had to be implemented with that library that didn't work with Passports. Will try again ,no promises.
TC: Implementation is not on the Broad's radar right now.

Plenary workshop
AP: Homework?
KR: None needed. Really would like WES folk there to discuss how they could use it.
FL: [Action] Check xSDO agenda and see if the AAI Passports workshop could be postponed to allow Cloud WS members to attend.

2022-09-08

Attendees - Tom Conner (Broad), Heidi Sofia (NIH), Martin Kuba (ELIXIR-CZ), Max Barkley (DNAstack), Michele Mattioni (Seven Bridges)

Actions

Actions Arising	Assigned To	Deadline

Previous Actions

- [ ]

Minutes

No discussion

2022-09-01

Attendees - Tom Conner (Broad), Kurt Rodarmer (NIH), Heidi Sofia (NIH), Martin Kuba (ELIXIR-CZ)

Actions

Actions Arising	Assigned To	Deadline

Previous Actions

- [ ]

Minutes

Discussed possibilitiy of demonstrating 1.2 implementation prior to plenary. Nobody on the call believes it will be achievable to have a fully running implementation with token exchange ready to show.

2022-08-25

Attendees - Name (Affiliation): Fabio Liberante (GA4GH),
Kurt Rodarmer (NIH), Tom Conner (Broad), Heidi Sofia (NIH), David Bernick (Broad)

Actions

Actions Arising	Assigned To	Deadline

Previous Actions

- ☑ ~~Introduce deprecation warning~~

Minutes

KR: FHIR/dbGaP not ready in time. Will have to do everything through publicly accessible. Nothing with FHIR. Maybe a recording of FHIR? In the absence of FHIR, being able to authenticate tokens and use them against DRS. Our DRS is taking this derived token already. It just forwards this token to the Clearinghouse.

Not my goal to raise this as a challenge. The approach is there. How does it affect downstream work that GA4GH is doing? Will at least discuss what the WOT is capable of doing. Different responsibilities than a Passport. Ensure that computation is geographically limited. Spark imaginations. What could you use it for?
FL: DUO implications?

KR: Provides technical control.
KR: Many people think of Passport as their personal capabilities. What's missing from imaginations, they are giving out their car keys to attendants. You are in control, but should be careful about what you hand out. Control over the researcher.
DB: Risk assessment before handing out keys anyway. Semi-vetted third party.
KR: Difference between trusted and trustworthy. Safer if you can complete all your analysis without trust. Expose vulnerabilities.
TC: It's a conscious decision.
KR: Human relationships as analogies get difficult. Security levels are granted to people who may not need it.
DB: Zero trust is preferred, but the question is if this is achievable in genomics.
KR: More about reduction.
HS: Attack surface reduced/quantified.
TC: Bounds trust, time etc.
KR: Valet does the same job with the car key or all keys.
DB: ABAC - attribute based authorisation.

KR: v1.2 requires custom visa in RAS (also custom in v1.1) - will prefer it to be opaque for v1.2. Issuer and consumer and nothing in between. NIH dbGaP specific.

[see recording 36 minutes in]

KR: Would require more relationships between service and consumer.

2022-08-18

Attendees - Name (Affiliation): Tom Conner (Broad), Kurt W. Rodarmer, Heidi Sofia (NIH), Christopher Siwy (NIH), Andrew Patterson (UMCCR/BioCommons)

Actions

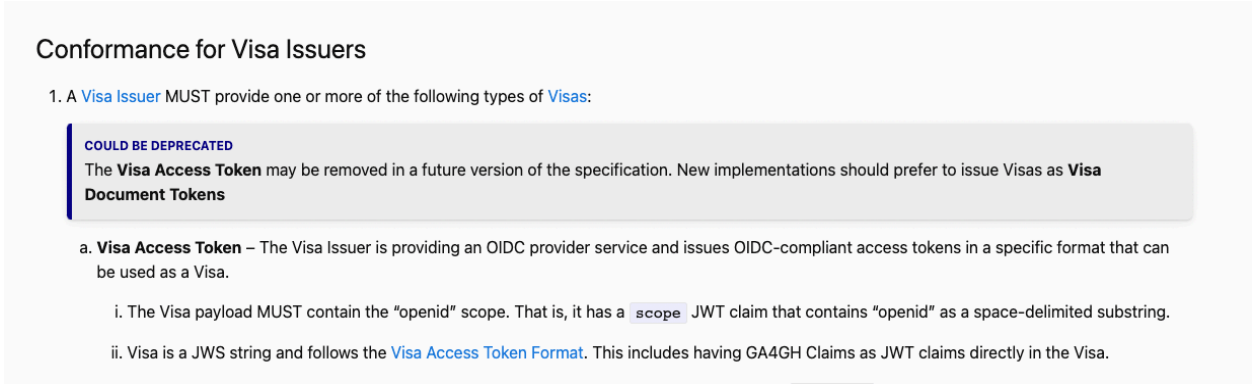
Actions Arising	Assigned To	Deadline
Introduce deprecation warning	Patto	Next week

Minutes

MB: https://github.com/ga4gh/data-security/pull/85/files (removed ~~Access tokens MAY contain non-GA4GH Claims directly in the access token.~~)

AP: Not explicit about Passport having GA4GH claims elsewhere.
MB: Should have it somewhere. Move to "Passport-Scoped Access Token issued by Broker" section.
No objections
TC: Happy to review.
MB: https://github.com/ga4gh/data-security/pull/84 - change label for arrow. "Provide Passport and Visas"? Covers 1.0 & 1.2.
AP: +1

AP:
Anyone want me to do this? CSS callout for deprecation. Don't want to miss the marker.



TC & MB: +1
MB: Deprecated, but not removed. Java language.
MM (in chat):*From Django policy "A feature release may deprecate certain features from previous releases. If a feature is deprecated in feature release A.x, it will continue to work in all*

A.x versions (for all versions of x) but raise warnings. Deprecated features will be removed in the B.0 release, or B.1 for features deprecated in the last A.x feature release to ensure deprecations are done over at least 2 feature releases."
AP: Deprecation warning - in orange and make a note in the changelog.

AP: What happens if a clearinghouse receives a Visa it doesn't recognise?
KR: NIH - they are specifically ignored. No requirement to recognise them. NIH isn't allowing recpackaging of the Passports anyway, so moot point.
AP: A visa that I trust the issuer and the visa itself, but it's expired. Do we have the same response for all categories, expired, unknown issuer etc.
MB: Spec vaguely tells you what to do if it's expired. Revocation section. Reasonable expiration periods. Doesn't specify e.g. 401 response etc.
AP: What happens to the Passport if one of the
[13:19]
KR: Only look at expiration date of visas we recognise. Assuming we accept the sig, we would look at the passport and the visa has expired, we would reject the whole thing. An issuer should be capable of checking that first. Otherwise it's suspicious. All the time on the shape of the tokens. Not the main purpose of what we're trying to do. The Clearinghouse is
MB: My biggest thing when reading through the whole spec, compared to RFC. The overall interaction and then the details of them, response status etc. Our Intro/FAQ and diagram could move to the start of the Intro. Structural improvements for 2.0.
AP: Balance non-normative with legibility. Maybe make non-normative sections clearer. 2.0 time frames.

MB: Can we update the Google Doc? Tag the Google Doc versions between.
FL: To do - update Google Doc after MB PR.
MB: To email when done.

2022-08-11

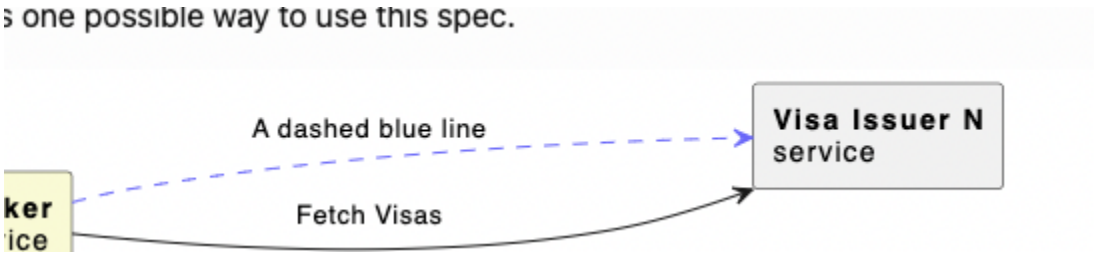
Attendees - Name (Affiliation): Fabio Liberante (GA4GH), Kurt Rodarmer (NIH), Max Barkley (DNAstack), Michele Mattioni (Seven Bridges), Martin Kuba (ELIXIR-CZ)

Active Github branches
https://github.com/ga4gh/data-security/tree/1.2-draft-main
https://github.com/ga4gh/data-security/tree/1.2-draft-max-intro
Branches published on web
https://ga4gh.github.io/data-security/1.2-draft-main/
https://ga4gh.github.io/data-security/1.2-draft-max-intro/aai-introduction

Apologies from Patto
Minor list styling PR https://github.com/ga4gh/data-security/pull/83

Jekyll update is close - waiting on their next release (issue added to our repo)
Got about half way through top-to-bottom review - only finding minor formatting issues - will do the rest next week. Not finding anything worth holding up external review.

I can't remember if we still needed it - but there didn't seem to be any issues with dashed or coloured lines for Jekyll.




```
Broker -[#6666ff,dashed]-> IssuerN : A dashed blue line
```

Actions

Actions Arising	Assigned To	Deadline

- *Work Order Token workshop at Plenary - now 15:00-17:00 - virtual as backup.*
- *Poster? - Depending on effort.*
-
- *Clarification around implementations - KR: Misinformation. RAS is difficult to define. Authorization vs Identification. dbGaP - working DRS. Moving on FHIR. Not a prototype. Disinformation. The Plenary? Plenary documentation.*
- *MK: List of known implementations - third other than ELIXIR and RAS. MB: DNAstack Broker for Beacon network and MSSNG (part of Autism Speaks driver project)*
- *MK: Question around v1.2 implementations.*
- *MB: Maybe for Autism Sharing? Not clear.*

- *KR: dbGaP prototyping - available for evaluation. Some changes that may take time to adapt to. Push to open spec for Visas. NIH custom Visa. Problem is Visas are open. For 2.0 it will be opaque. 1.2 clients will have to dance to that. The token for the visa will be considered opaque in 1.2 implementation. An adjustment to spec, but not off-spec. Should have always been opaque. Every time we make a change - every single endpoint needs to change. Not secret, commitment to interpretation.*
- *MK: A bit lost. NIH will implement 1.2, but?*
- *KR: NIH complicated. Don't just decide to put it into production. Prototype and convince remaining institutes that it will be worth it. Institutes individually funded.*
- *MK: Broad Institute implementation relation to RAS?*
- *KR: Complicated. Broad & UoChicago. UoC provides main interface for others.*
- *MM: Seven Bridges - worked with UoC - dbGaP access pre-RAS. Worked to integrate with RAS. UoC first milestone one. Now each implementation wants to interact with RAS directly. Building clients. Currently, working to getting production credential for RAS. Depends on where the data is actually sitting. Different type of implementations, in different stages of development. Still using the old version.*
- *KR: +1*
- *MM: For passport 1.2 - if we are working with RAS/dbGaP - ability to get to the data. If they are going to adopt 1.2. We will have to as well.*
- *MK: Implementations of?*
- *MM: Broker or Clearinghouse.*
- *KR: Visa Issuer is dbGaP. Our CIT group access the Broker and issues the Passport. In-house. The Clearinghouse, multiple dbGaP, UoC has their version of Clearinghouse. MM can get a passport from RAS CIT group and can send it to a RAS dbGaP server. And return a URL to data.*
- *MK: What to the Brokers do?*
- *KR: NIH governed data are stored in several hosting environments. Not just NIH premises. NIH issues tokens. CIT as the Broker. We issue tokens to data wherever it lies. What about repackaging? Difficulty with that - Visas being bearer tokens, stored by a Broker for reissue - a break in the chain of authority. Not related to an authentication event. Packaged into indivisible form to prevent this. Craig was working with me on approaches to fix that - dropped off.*
-

Previous Actions:

- ☑ ~~Check PlantUml arrow/line/colours - maybe bump version~~
- ☐ Adjust preamble in Google Doc for review
- ☐ Read AAI top-to-bottom
- ☐ Read Passports
- ☐ Gather slides/links for PRC

Minutes

Provide visas and switch arrow direction in Intro diagram. **Last thing before PRC.**

Links in Passport to AAI specification - depends URL.

MK: Merge main draft into master?
MB: GA4GH links to master?? Yes,
https://www.ga4gh.org/news/ga4gh-passports-and-the-authorization-and-authentication-infrastructure/ links to master branch.
MK: Wrong to link to master in blog post. Should use the tag.
MB: If merge draft branch into master, a link at top of readme for tags/branches.

Hard deadline next Thursday - for PRC sharing.

2022-08-04

Attendees - Name (Affiliation): Fabio Liberante (GA4GH), Max Barkley (DNAstack), Tom Conner (Broad), Kurt Rodarmer (NIH), Andrew Patterson (UMCCR/BioCommons), Christopher Siwy (NIH/ODSS)
Apologies:

Active Github branches
https://github.com/ga4gh/data-security/tree/1.2-draft-main
https://github.com/ga4gh/data-security/tree/1.2-draft-max-intro

Branches published on web
https://ga4gh.github.io/data-security/1.2-draft-main/
https://ga4gh.github.io/data-security/1.2-draft-max-intro/aai-introduction

Actions

Actions Arising	Assigned To	Deadline
Check PlantUml arrow/line/colours - maybe bump version	Andrew	Next meeting
Adjust preamble in Google Doc for review	FL	
Read AAI top-to-bottom	TC/AP/MB	
Read Passports		
Gather slides/links for PRC	FL	

Previous Actions:

- [x] ~~Introduction - restructure and amend diagram~~
- [ ] Read through AAI 1.2-draft-main top-to-bottom to find what's left to work on
- [ ] Read passport spec to see what's left

Invitation to Work Order Token workshop at Plenary

Minutes

MB: Intro changes.
TC & AP: Comments in Github
TC: Wording suggestion change - remove "request public key" arrow
MB: Wanted to show some kind of connection between Clearinghouse and Visa Issuer - wanted a dotted line - show dependence. E.g. "validates visas from"
KR: Separate box to show Clearinghouse consumes what Visa Issuer produces. Explicit statement that states what relationship is.
MB: Yeah, maybe. Even dotted arrow could be confusing.
TC: Can validate signature offline - arrow would confuse that use case.
KR: Difficulty with RAS with people not understanding transfer of information/visa through middle.
MB: Just remove the arrow for now. Prioritise spec?
TC & AP: +1
MB: Checking through Github comments.
AP: Service word is redundant. MB:+1
AP: Individually signed attributes. Core thing is that they are signed claims. Not just JWTs with JSON. Signed researcher attributes.
MB: Spec defines cryptographically signed attributes. AP:+1
TC: "Ubiquitous not pervasive." comment MB: Commit
https://github.com/ga4gh/data-security/pull/80/files#r937364392
AP: Spec diagram was ¾ not stuff in the spec.

TC: Move it into FAQ?
MB: +1 for liking diagram.
AP: Leave in spec for the moment. Will check plantUML rendering.
MB: All comments through. Tom review?
TC: Doing now. Complete.
MB: Will do top to bottom review.
AP: Will do “printed” review.
MB: Merged.
MB: Review Passport spec.

AP: AAI Connect diff between branches won’t even render.
MB: Martin’s Summary of changes is good but complex - stick to two things. Slide deck from Connect in April. Maybe even use that presentation?
TC: David would probably read it fresh anyway.
AP: Rendered versions of the branch.
MB: For Data Connect used Google Docs. David would probably be fine with Github comments.
MB: Pull request as merge to draft for David to review? Very messy. Could be good way for comments.
TC: Paste it into Google Doc? Terrible idea.
AP: Plausible. Track changes and then PRs?

AP: I’ll check PlantUML - Google Docs.
MB: Slide 15 is summary Montreal 2022 Connect Passports Workshop Check it’s still accurate.
TC: There is a summary.
MB: Mechanical. Not order of importance.
TC: Pasting spec into Google Docs. Doesn’t look so bad. Open question.
AP: Master Google Doc and fix tabs - then a specific copy for each reviewer.
MB: When shall we share with David Glazer? Still missing a once over. Share it with David next week? Depends on everyone else. I think I can on Tuesday. Try to get issues resolved before Thursday.
AP: I can.
TC: I can.

GA4GH Data Security -- AAI Profile -- 1.2 Draft Main Branch - Tom Conner is the owner. Transferred to FL.

TC: Changelog was deleted from document.
FL: Stick with Github until next week.
MB: Warning at top of document that it is for comment only.
AP: Link to rendered.
TC: Link to PR too.
TC: Profile document only - rest of AAI v1.2 elsewhere.
TC: Fabio to adjust preamble.

2022-07-28

Attendees - Name (Affiliation): Tom Conner (Broad), Max Barkley (DNAstack), Kurt Rodarmer (NIH), Michele Mattioni (Seven Bridges), Christopher Siwy (NIH), Fabio Liberante (GA4GH)

Apologies:
Andrew Patterson

Active Github branches
https://github.com/ga4gh/data-security/tree/1.2-draft-main
https://github.com/ga4gh/data-security/tree/1.2-draft-faq-key-management
https://github.com/ga4gh/data-security/tree/1.2-draft-max-intro

Branches published on web
https://ga4gh.github.io/data-security/1.2-draft-main/
https://ga4gh.github.io/data-security/1.2-draft-faq-key-management/aai-faq
https://ga4gh.github.io/data-security/1.2-draft-max-intro/aai-introduction

Actions

Actions Arising	Assigned To	Deadline
Introduction - restructure and amend diagram	MB	

Previous Actions:

- [x] ~~Check with web dev about URL/file hosting~~
- [x] ~~Introduction editing/drafting~~
- [x] ~~Might want FAQ entry on different kinds of visa issuers (ones that are OIDC providers versus minimal issuers)~~
- [x] ~~FAQ entry on key management (possibly combined with above)~~
- [ ] Read through AAI 1.2-draft-main top-to-bottom to find what's left to work on

- [ ] Read passport spec to see what's left

MB - Rich diff for Intro edits - https://github.com/ga4gh/data-security/pull/80/files?short_path=b3784b2#diff-b3784b2123021343168458c702282137e69abaf062fe9b24c86d6b293e10c500
Cut text for intended for Driver Projects - should be an open standard.
Reword second paragraph.
Broker chaining was emphasized more than it has actually been used.
How separate data holders and controllers
KR: Maybe improvements to the definition of Data Holder and Controller? "Enforcing access" is confusing -
MB: Language from specifications? Test links to definition https://ga4gh.github.io/data-security/1.2-draft-max-intro/aai-introduction - organisation that protects a specific data?
KR: It holds and serves data - protect is where it gets sticky. Shared burden. Interpretation of responsibility of protection.
MB: Organization that hosts data while respecting Controllers policies?
TC: +1
FL: Should we redefine in Spec? Currently *"Data Holder – An organization that protects a specific set of data."*
TC & MB: +1

MB: Background - removed examples of Broker technologies. None of these are GA4GH Brokers out of the box.
KR: +1
TC: Covered below. Avoid listing specific players.
KR: How did NIH/VDS get in there?

KR: The idea of a "lego" model with different IdPs. That's a major policy issue. A Google account doesn't mean you're in.
MB: Main slant of the intro was that you could interact with multiple IdPs - which isn't the case.
KR: At the beginning of this - Brokers wrote it as Broker centric - ultimate goal is repository centric.

MB: Embedded tokens too heavy for Intro. Visa Tokens Explanation more concise, less technical.
KR: Google referenced a lot.
MB: Will strike second Google reference.
MB: Simplified flow diagram.
KR: Vote to remove chaining idea. 3rd Party brokers.

MM: Not clear what the Visa Repository is.
MB: Simplify diagram to remove repository.
MM: Agreed - emphasize the right hand side.

MB: Will make these changes. Make unspecified clearer.
MB: Revisit chaining issue.
KR: Wording in search of an example use. Also, the diagram isn't clear. Authentication is only the beginning of the journey. Once the Broker has done its thing - it's between the Clearinghouse and the data.
MB: Diagram should reflect the 3 part makeup rather than boxes suggesting all part of one process.
TC (in chat): *Same diagram is still in the profile with a paragraph about it: https://ga4gh.github.io/data-security/1.2-draft-max-intro/aai-openid-connect-profile#flow-of-assertions*
MB: Will revisit Why Brokers section.

MB: Future topics to explore - maybe in readme or somewhere else. Visa Tokens Explanation
TC: Remove the explanation from the title. Link to Visa and Visa Issuer definition?
MB: Each term is linked to definition the first time it's used.
TC: Visa should be at the top.
KR: The order is backward. The Visas are the important thing.
MB: Will ping on Github for changes.

2022-07-21

Attendees - Name (Affiliation): Max Barkley (DNAstack), Kurt Rodarmer (NIH), Heidi Sofia (NIH), Fabio Liberante (GA4GH), Michele Mattioni (Seven Bridges), Martin Kuba (ELIXIR-CZ),

Apologies:

Actions

	Actions Arising	Assigned To	Deadline
	Check in with Andrew around Visa Issuer FAQ	Fabio	

Previous Actions:

- [ ] Check with web dev about URL/file hosting
- [ ] Introduction editing/drafting
- [ ] Might want FAQ entry on different kinds of visa issuers (ones that are OIDC providers versus minimal issuers)
- [ ] FAQ entry on key management (possibly combined with above)
- [ ] Read through AAI 1.2-draft-main top-to-bottom to find what's left to work on
- [ ] Read passport spec to see what's left

Minutes

2022-07-14

Attendees - Name (Affiliation): Andrew Patterson (UMCCR/BioCommons), Tom Conner (Broad), Martin Kuba (ELIXIR-CZ), Max Barkley (DNAstack), Fabio Liberante (GA4GH), Kurt Rodarmer (NIH), Christopher Siwy (NIH), Heidi Sofia (NIH)

Apologies:

Actions

	Actions Arising	Assigned To	Deadline
	Check with Web Dev	Fabio	
	Introduction	ALL	

Previous Actions:

- [ ] Might want FAQ entry on different kinds of visa issuers (ones that are OIDC providers versus minimal issuers)
- [ ] FAQ entry on key management (possibly combined with above)
- [ ] Read through AAI 1.2-draft-main top-to-bottom to find what's left to work on
- [ ] Read passport spec to see what's left

Minutes

KR: Discuss WorkOrder Token today briefly?
AP: Who is going to Plenary?
MK, TC, MB, KR, MM?

AP: WIP. To be reviewed. Happy for other input.
MK: I approved.
MK: Which URL still open?
AP: Passports & AAI are still separate. Not trivial.
TC: For v2.0?
MK: We want stable links.
AP: Could bite the bullet? Github vs web host. Or ReadTheDocs? VRS/Pedigree/Phenopackets. https://pedigree.readthedocs.io/en/latest
MB: If not domain - just stick with Github

AP: Introduction needs work.
MB: Two hackathon sessions. WorkOrder Token session and DRS/Passports Integration session. Timings to go onto swoogo site. *DRS & Passports times that are currently planned:*
** July 20, 10-11AM EDT*
** July 27, 9-10AM EDT (overflow time if needed)*

MM: Is anyone from RAS joining DRS/Passports?
KR: Chris, anyone? CS: I probably will. And share it around with the RAS Project Team. HS: +1
KR: DRS server running for many months now.

KR: WorkOrder Token presentation.

- Prototype working.
- Two complaints about Passports
  - 1 - self-contained RAS Passports is bulky, especially if you are a power user - difficult to manage and precludes use in legacy systems that expect single token and header.
  - 2 - used a Bearer Token when it should be Assigned. And this you shouldn't drop it to disk. Makes command line work difficult.
- WOT intends to be Assigned - less volatile. Cannot be used by others unless they can prove identity or a certain environment that was approved for its use.
- WOT (aka Task Specific Token) can be derived from the RAS Passport subset. Will eventually be automated as part of the discovery process.

- Tokens are informationally equivalent, but <10% of the size. 6,177 vs 500 bytes.
- Started prefixing token with a tag to identify type of token - at least what it claims - before verification.
- Clearinghouse has been updated to accept this new Token.
- Would like to go over this graphically at some point - September?
- Assignment stuff may increase the size marginally.
- SRA toolkit - obtains a token that is only accessible via GCP.
- Can compare constraints between tokens - e.g. a particular Google environment.
- How can this constrain access to certain regions of the cloud? European continent limitations etc.

AP: 3 assignments, identity etc? So the token would support different constraints?
KR: Contract between Visa Issuer and the Consumer. Types of constraints may not be universal. May be particular to a repository. Initial focus on cloud environments or individuals. Task Specific Token should last longer than minutes. RAS team 12 hours, but 15 days with renewal. One token to solve too many problems. NIST considerations go away if the token cannot be used to say that the user is there and alive. Enables long running batch jobs. Could be renewed by the process that is using it. Revocation built in.
MB: Next Thursday 9am EST Hackathon. As KR's work is the main prior art - would be good if you could join?
KR: Who else is there outside of NIH?
MB: Martin and Ian.
KR: Will demo to dbGaP group today. Probably want a bigger RAS team presentation too. Live demo at Barcelona.
MB: Keep current plan for Hackathon.

KR: RE Barcelona - workshop type thing seems more appropriate. HS: +1.

2022-07-07

Attendees - Name (Affiliation): Max Barkley, Tom Conner, Martin Kuba, Heidi Sofia, Andrew Patterson

Apologies: Fabio Liberante (GA4GH)

Actions

	Actions Arising	Assigned To	Deadline
	Might want FAQ entry on different kinds of visa issuers (ones that are OIDC providers versus minimal issuers)	Andrew	FAQ entries have been written and some feedback processed.
	FAQ entry on key management (possibly combined with above)	Andrew	
	Read through AAI 1.2-draft-main top-to-bottom to find what's left to work on	Max	
	Read passport spec to see what's left	Max	

Minutes:
Discussion of several pull requests in the AAI repo.
Discussion of the large pull request in DURI.

2022-06-30

Attendees - Name (Affiliation): Max Barkley (DNAstack), Fabio Liberante (GA4GH), Tom Conner (Broad), Martin Kuba (ELIXIR-CZ)

Apologies: Andrew Patterson (UMCCR/Biocommons)

AP - Notes ahead of meeting
I have added a threat analysis diagram to the FAQ.
I have applied Max's feedback to the sequence diagram.
Styling <hr>s have been applied and merged (please check to make sure the sections have not changed level accidentally)

Actions

	Actions Arising	Assigned To	Deadline
	Contact Jon Turner about sub-domains	FL	
	PR reviews	ALL	

Previous actions

- [ ] Check with Susan on moving GitHub
- [x] ~~Grant DURI GH access in the meantime~~
- [ ] Contact PRC candidates
    - [ ] Shortlist first
- [x] ~~FAQ~~
- [x] ~~Styling of document (low priority)~~
- [x] ~~Passports spec MIME type~~

Minutes

FL: Query around where PP spec lives. Github Repo.
MB: Makes sense to coincide with a release.
TC: AP had suggested a top level URL. I suggested versioning in URL.
MK: Github Repo/IO etc?
TC: Run Jekyll and push to domain.
MB: Older versions of spec had Github pages. But not standard linking - published pages or markdown? Which is the official standard - the published or the raw markdown?

MK: Should be the published official URL is stated in the beginning of the document. Latest version is always linked. We just **need final URL**.

Github now has “rich diff” feature

NB: MTLS - is to mitigate certain attacks.
TC: Not part of the specification.

MB: Aud resource extension changed by AP. Approved. DRS example included and Threat Analysis.

MK: Styling changes ok. PR needs approved and can be merged.
MB: Changing PR status.

MK: Changed MIME type in Passports spec.
https://github.com/ga4gh-duri/ga4gh-duri.github.io/pull/57
TC:
https://github.com/ga4gh-duri/ga4gh-duri.github.io/pull/57/files#diff-01d3c4ec1e325d3bd2071e7b9dfe835598070726d7232a0ceedfe329de3e6851

MK: New PR to correct missed changes. E.g. Claim Clearinghouse → Passport Clearinghouse. Also added broader recommendation for PKCE. Conformance for Brokers - repeating OIDC - replaced with reference to OIDC spec, which is linked elsewhere in the document. Limited damage of leaked (Passport Scoped Access Token) tokens recommends a time limit. I would recommend a refresh token rotation. OIDC landscape has changed, so this brings it more in line with the current security situation.

MK: Anything else?
MB: Fresh read?
MK: Could still be shortened?

2022-06-23

Attendees - Name (Affiliation):
Andrew Patterson (UMCCR/BioCommons), Martin Kuba (ELIXIR-CZ)

Actions

	Actions Arising	Assigned To	Deadline
	Check with Susan on moving GitHub	FL	
	~~Grant DURI GH access in the meantime~~	~~FL~~	
	Contact PRC candidates	FL	
	FAQ	ALL	
	Styling of document (low priority)	ALL	
	Passports spec MIME type	MK	

Previous actions

- [ ] Links in Passport
    - [ ] Need access to Github
- [x] ~~Remove Implicit Flow~~
- [x] ~~Paragraph around signing algs~~

TC: AUD claim not changed.
KR: AAI 1.0 GA4GH def of JWT and scopes required. Purpose not clear if visas are loose.
MK: Only in Access Token. Nobody uses this part anyway. Was not req in
KR: Stipulated at the level of JWT conformance? Not sure.
TC:
AP: Access token must have OpenID - Visa Document must not. Header makes it unclear. Change order? Order changed in FAQ already.
Agree with AUD claim conclusion in previous meeting. However, it may have benefits.
MB: Maybe in FAQ - or spec. Possibly list RFC extensions that could be allowed?
AP: Will make Token Exchange leaner and include audience stuff.
MB: Query sig algs PR. Language is still ES256/RS256, did we not want to allow more secure algorithms in future?
TC: Back and forth.
MK: Kurt objected on grounds of compatibility.
MB: PS256 was recommended in the blog article.
MK: This was only for encrypted tokens.
TC: Article is about encryption. Do we be more explicit about that in the spec? Currently links to best practices document. Even if some details are irrelevant.

MB: I don't feel that strongly about it.
TC: If the worst happened - people would rush to fix that anyway. We could do it ourselves in future.
KR: <b64> claim. Claim that allows you to specify if base64 or verbatim/binary payload, boolean value.
MK: Can it be used for tokens?
KR: Yes.
MK: Does this happen for tokens or signatures?
KR: I'll check, but JWS/JWE moved after the original spec.
MK: JWT specifies that it must be encoded. Not much choice.
KR: JWS not JWT. JWS (3 parts) or JWE (5 parts). This matters. Can be 5 parts.
MK: Only if encrypted.
KR: b64 is specified at JWS/JWE level, but not part of JWT. Are we leaving out b64?
TC: Shouldn't restate every detail in other specs. Have been selective. Will merge once approved.

MK: Github pages vs source code links? Which for the next version? Generates TOC!
https://ga4gh-duri.github.io/researcher_ids/ga4gh_passport_v1.html

AP: I agree with the rendered version. Can we move to GA4GH GitHub? If moving and breaking other links anyway.

KR (in chat):Okay - RFC-7797 "updates RFC 7519 by stating that JSON Web Tokens (JWTs) MUST NOT use the unencoded payload option defined by this specification."
So JWTs are not affected. Sorry for the noise.

MB (in chat): FYI, this was the quote I was thinking of about required RSA algorithms: "Although no attacks are known against RSASSA-PKCS1-v1_5, in the interest of increased robustness, RSASSA-PSS is REQUIRED in new applications." html/rfc8017#section-8

AP: Good edit to split sections. Pleased with the changes! Introduction?
FL: Not yet.

MK: PP spec defines visa. Should we change the JWT media type to be more specific? In JWT header. Type claim.
AP: Not a MIME type, but a token type.
MK: Almost the same.
MB: Word it as recommended, but not required.
KR: Fear that off the shelf libraries might not be compatible.
MK: Clearly identifies token type.
KR: Most of understanding is from token content itself.
AP: More important as token types proliferate in spec.
TC: How could one hack it? There may be ways, but in favour of specific type.
AP: Helps with debugging. System shouldn't blindly accept type anyway.

MK: Edit PR to use old one or recommended new one.
MB: Type is only applicable to Visa Document format. As the other hopefully goes away in the next major revision.

AP: Timeframe? September Plenary? When do we share it more broadly.

TC: We have a list of relevant specs. External links are fine as is. DURI links WILL have to be updated. That's just a mechanical change.
MB: Based on content changes. **Beginning of August? Soft deadline.** Leave styling to the end.

FL: PRC suggestions? See draft approval document.

Outstanding actions

- ☐ FAQ
    - ☐ Group Review
- ☐ Styling of sections
- ☐ Passports MIME type visa
- ☐

2022-06-16

Attendees - Name (Affiliation): Max Barkley (DNAstack), Tom Conner (Broad), Csaba Halmagyi (EMBL-EBI), Martin Kuba (ELIXIR-CZ), Fabio Liberante (GA4GH)
Apologies - Andrew Patterson (UMCCR)

Actions

	Actions Arising	Assigned To	Deadline
	Links in Passport	MK	
	Remove Implicit Flow	TC	
	Paragraph around signing algs	TC	

Patto: I have started on a FAQ branch
https://github.com/ga4gh/data-security/pull/73

published to
https://ga4gh.github.io/data-security/1.2-draft-faq-changes/
(for some reason the publish builds on github actions randomly fail for me)
Absolutely completely just brain dumps (and the sequence diagrams from before) - feel totally free to re-organise / re-word / delete - I will not be offended! Just make changes directly on the branch.

Previous actions

- [ ] Make a <hr/> PR with varying levels of hrs between headers - and bump all the header levels up 1.. I.e ### -> ## (currently header level 2 is never used and header level 6 is used - but isn't really a header when rendered)
- [ ] ~~Replace MUST with SHOULD for RS256 & ES256 - see RFC8725~~
    - [ ] RS256 ok for signing but not encryption
    - [ ] ES256 ok -
    - [ ] Best EdDSA is not supported yet
    - [ ] List of supported algorithms
- [ ] Add SPA/auth-backend example in FAQ
- [ ] Remove prescription for OIDC Implicit Flow (
- [x] ~~Issue created for FAQ~~
- [x] ~~Collect ideas for FAQ~~

MK: Internal vs External link changes should be in Passport not AAI spec. I will do this.
MK & TC: Single link to definitions.
TC: All agree that mandating Implicit Flow is less secure, especially for SPA.

DEPRECATION WARNING in spec itself under UserInfo

FAQ
https://ga4gh.github.io/data-security/1.2-draft-faq-changes/aai-faq

- End to end flow using /userinfo
    - Title implies that this end-to-end flow is the preferred
        - "Preferred v1.0 flow" vs "Token Exchange flow"
        - Or change the order? TC&MK
    - omit part with parentheses (plain JSON, not signed JWT)
    - "Passport content" → "asks UserInfo for list of visas"
    - Passport doesn't exist in the userinfo flow
    - "Client is given data" - data provider is expected to be Clearing House.
    - Move UserInfo into Legacy?
    - Should you use the signed JWT? DEPRECATION WARNING.
    - UserInfo returning a signed JWT is possible, but not recommended as an access token to access data.
- Token Exchange flow
    - Oxford spelling - Authorization.

    - Use of ** for italic text in diagram? Should use //italic// in PlantUML - https://plantuml.com/creole
    - Aud - audience claim? - not mentioned in spec. OAuth RFC ext allows this. Current spec says `aud` optional in <Passport Payload> but MUST NOT include `aud` for <Visa Access Token Format>.
    - {REPLACE WITH CORRECT DRS DETAILS} - added passport attrib to POST request to access data. MB to make a request in the PR.
      Client requests data needs an example request.
    - ELIXIR approach is “Beacon” to be able to search only data a user would have access to.
    - https://github.com/ga4gh/data-security/pull/73/files
- Move “Can a JWT alone be used for authentication even if the spec mostly talks about OIDC Flow?” to Legacy? MB & MK
- Threat Analysis diagram - MB will make some suggestions in Github
- SPA diagram - check grammar/punctuation
- Remove “Can the output of /userinfo be used as a JWT for Authentication?” entirely

2022-06-09

Attendees - Name (Affiliation): Max Barkley (DNAstack), Tom Conner (Broad), Martin Kuba (ELIXIR-CZ), Christopher Siwy (NIH), Kurt Rodarmer (NIH), David Bernick (Broad), Heidi Sofia (NIH)
Apologies - Andrew Patterson (UMCCR) - some pre meeting notes below

Actions

	Actions Arising	Assigned To	Deadline
	Make a PR with varying levels of hrs between headers - and bump all the header levels up 1.. I.e ### -> ## (currently header level 2 is never used and header level 6 is used - but isn't really a header when rendered)	Patto	Once we are close to closing off the changes to 1.2-main - the change is purely cosmetic
	Replace MUST with SHOULD for RS256 & ES256 - see RFC8725	TC	
	Add SPA/auth-backend example in FAQ	MB	Added to Issue for FAQ
	Remove prescription for OIDC Implicit Flow	TC	
	Issue created for FAQ	Done	
	Collect ideas for FAQ	ALL	

Agenda

	Agenda Item	Person/Time
1		
2		
3		
4		
5		

Previous actions

- [x] ~~Follow up with suggestions on passport token PR~~
- [ ] PR for client/application conformance

- ☑ ~~Look into options for token exchange for SPA~~

  Patto: I have looked into this - I think the consensus from KR/MB that pure SPAs are probably not suited to do token exchange safely is true (no easy way of proving token has not leaked and exchange is being done with authorised client) and I reworked my SPA to be a combined SPA + auth backend - and that's working well and can do token exchange but with proper proof of client identity. So I don't think there is any immediate issues here that need addressing in 1.2.
- ☐ Follow up on registration of URN
- ☐ Create issue to fix clearinghouse post 1.2
- ☐ Look into changes to intro and FAQ (addressing motivation of changes brought up by Christoph)

Questions from FL

- JWKS appears undefined - does this matter?
- Discussion with Discovery WS - could we use/encourage GA4GH ServiceInfo endpoint to allow the client to discover AAI version and token exchange support etc.? GA4GH service-info specification.
- Is there a reason <"ES256"> was added to signing algs? Will most clients be able to handle either algorithm?

Questions from Patto

- Would like at some point a set of questions for FAQ (if not answers - can start with the skeleton PR that has the questions at least). Maybe some high level grouping for the questions (architecture / security considerations / threat analysis). Am happy to do but any guidance/starter questions welcomed
  - FAQ issue added by MB - collect suggestions here https://github.com/ga4gh/data-security/issues/68

Minutes

Previous actions

Latest PR from MB covered.

MK: Do we need to specify algorithms?
KR: When you allow participants to use whatever you want, then you have a problem with client support.
RS256 - a vulnerable algorithm - should not use MUST

OIDC - with Implicit Flow should be PKCE instead.

URN registration - MK awaiting response see https://github.com/ga4gh/TASC/issues/36

Issue for FAQ questions

Future idea - JWKS extensions for key expiry and certs for validating the keys.

2022-06-02

Attendees - Name (Affiliation): Max Barkley (DNAstack), Andrew Patterson (UMCCR), Tom Conner (Broad), Martin Kuba (ELIXIR-CZ), Kurt Rodarmer (NIH), Nikola Stanar (Seven Bridges), Binam Bajracharya, Christopher Siwy (NIH)

Actions

	Actions Arising	Assigned To	Deadline
	Follow up with suggestions on passport token PR	Max Barkley	
	PR for client/application conformance	Tom Conner	
	Look into options for token exchange for SPA	Andrew Patterson	
	Follow up on registration of URN	Martin Kuba	
	Create issue to fix clearinghouse post 1.2	Tom Conner	
	Look into changes to intro and FAQ (addressing motivation of changes brought up by Christoph)	Tom Conner	

Agenda

	Agenda Item	Person/Time
i	Review MB's PR	
1	Actions from previous meeting	
2	Need for SPA/PKCE support?	
3	New token type URN	
4	Questions from Christoph Zwerschke	
5		

Previous actions

- ☑ ~~Reach out to AP about sequence diagram~~
- ☑ ~~Replace token type~~
- ☑ ~~Draft new token type spec~~

- [ ] Cleanup links across the spec
- [ ] PR in Passports Spec

Questions from FL

- JWKS appears undefined - does this matter?
- Discussion with Discovery WS - could we use/encourage GA4GH ServiceInfo endpoint to allow the client to discover AAI version and token exchange support etc.? GA4GH service-info specification.
- Is there a reason <"ES256"> was added to signing algs? Will most clients be able to handle either algorithm?

Minutes

Max's token definition branch (latest branch where action is happening)
https://ga4gh.github.io/data-security/1. 2-draft-passport-token-definition
https://github.com/ga4gh/data-security/pull/66

Open issues:

- Clearinghouse is too vague
  - Covers too many roles (pre-authorization clearinghouse, post-authorization clearinghouse fill different roles)
  - Potentially the right time to update this is when we work order token
- Maybe we need an issue on the data-security repo to track issues we want to address after 1.2

We did not get to FL question so hold them over to next meeting.

Minutes from Recording.

MB: UserInfo conforms to OIDC and then
AP: Extra text only necessary if we were saying that you can't get things signed. Just recommend token exchange.
MK: Is required compatibility with 1.0 written anywhere else? Should it be here that UserInfo can include the GA4GH Passport v1 claim?
MB: True. This is only the reference.
MK: Highlight that "For backwards compatibility this can contain the claim".
MB: +1. In the User Info definition be more specific about ga4gh_passport_v1
AP: Sequence diagram now pushed into MB's token-def branch.
MK: Signed visas can be sourced from multiple visa issuers or ~~visa assertion sources should be removed~~.
AP: Sorry for adding that. Added horizontal lines too.
MB: SPA?
AP: Christoph asked a broader question. I was querying token exchange generally requires an identifiable client. OIDC flow can be done with PKCE, but not with Token Exchange - according to spec.

AP: Everyone is using PKCE.
TC: Yeah, we gotta use PKCE. Shouldn't recommend something considered insecure.
AP: Implication of Token Exchange language - "Client authentication is required and that is done using PKCE for SPA." Unless we suggest doing Token Exchange with PKCE, but I don't see how you would do that.
KR: We have concerns about supporting SPA altogether. We have them, but do not use these approaches. Concern that they are supported or worse must be supported.
AP: Valid for an ecosystem not to support PKCE. Token Exchange current language rules it out entirely.
TC: Strike 2.1 & 2.2 under client application conformance? Security choices ought to be outside the spec?
AP: +1. Let's not be prescriptive in this spec. Whatever OIDC flow you want
TC: Alternative is to reference external security best practices? But simpler to eliminate section.
MK: Client application conformance - the first two points?
TC: Yes, and number
AP: Entire client application conformance could be an external best practice document.
MK: +1 - probably in an RFC.
TC: 5 refers to older RFC 6819 2013 document.
AP: Make reference to current RFC instead.
TC: Take a stab at finding an updated RFC to cover this. Discuss again
AP: This addresses PCKE & SPA at the OIDC flow end, but what about Token Exchange? Once my SPA has this Token and wants to do an exchange how do I prove to TE endpoint who I am? I authenticated as a client by PKCE, but how do you do that in a Token Exchange?
TC: I don't think there's a need for that.
AP: I have an SPA that I would like to do a flow through Broker and then make downstream API calls to an HTSget endpoint or something.
KR: Sticky areas with that. We started out saying that these would be bearer tokens for various reasons inc. simplicity. A security problem by keeping the tokens carefully managed. We at NIH keep tokens out of browsers and end user systems. Even though in theory and philosophy - the tokens are possessed by the user, we don't have the infrastructure to bearer tokens. Assigned tokens are a much better fit for this. Idea behind a work order token.
AP: I understand with concerns with bearers tokens in browsers. There is also a well-evolving way of doing this, Okta & Auth0 etc. Ruling out SPA is
KR: Not ruling that out. Just wary of any implication that it is ruled in.
AP: +1. Client authentication REQ - RECOMMENDED?
MB: OAuth RFC links to mechanisms other than client secret? Client assertion? Sign the JWT yourself. Your SPA could call a service to get an assertion. Important that we specify the importance of security.
KR: NIH uses SPA as MB just described. Security/authentication always goes through a server.
MB: Simplest thing is for just one endpoint to have a server for token exchange, but may not be palatable for logic in an existing SPA.
AP: I will investigate RFCs in this space.
MB: Check out client assertions. Imagine a scheme where every instance of a webpage has a generates key?

BB: What is the benefit of making it a requirement for making the application an SPA.
MB: That's not the case, we just want to leave the door open.

MB: New token type dealt with in the PR.
AP: Do we want to register in the namespace?
MK: Some committee for this, but it will take time.
AP: Not likely to find an equivalent GA4GH use of the names.
MB: Who should carry the flag for this? TASC?
MK: I will try to take care of this. I registered.

MB: Most of the questions from Christoph addressed in OIDC discussion.
TC: PR to clean up links. Ended up doing some edits in that based on Christoph's comments. Three things. 1. Broken links - MK caught. 2. Implicit flow - already discussed. 3. Cosmetic thing - changed a numbered list for a single item to bullets. Combine text with parent item. Already in a PR. Will wait for MB's PR first.

AP: Lots of "clearninghouse" typo introduced.
TC: I will check that.
MB: One other thing in Christoph's email. He asked about the motivation for Token Exchange. How or where do we think we include text around the motivation?
TC: Can't believe I forgot the biggest point. And the Intro definitely needs updated.
AP: The sequence diagrams could go into an FAQ or Appendix, they're non-normative. Perhaps you could include it there. Or an architectural decision register? Do we want that level of detail? There already is an FAQ.
MB: Intro & FAQ seem like a good idea. Not too much detail.
KR: Clearinghouse issue. A contentious concept, back to problems trying to solve last year. Clearinghouse for what? For a preauth token - will have different properties - OAuth model. Post-auth token - the OAuth model doesn't apply. Clarify naming around things - similar but separate concepts/implementations.
MB: Perhaps having adjectives in front of clearinghouse?
KR: Not sure. Existing descriptions all envision OAuth authorisation server. The way we envision it working post auth is that the auth token is of such value that it can't be subverted or replaced unless issued by the same authority. Any Clearinghouse that performs post-auth needs to be within the trust boundary - NIH define that as internal to the system itself. Importance of original authority. The point being what NIH sees as a Clearinghouse is not what is described. We don' share the view at all. We're going for a different thing. Good to describe that there are different components involved.
TC: Is this a change necessary in v1.2? Is Clearinghosue
KR: Leaving it as is is better for now. Work Order token is a better time to discuss. That is a post-auth device - so this idea can be described then. Trying to avoid being boxed in. Leave it as it is. We don't use the Clearinghouse in the way that it's described - maybe need to rename it.

MK: Agree, leave it as is and maybe totally remove it in v2.0? Or rename to Passport Consumer?
MB: We should keep a tally of things like this for v2.0. Where should we track this? Issue on the data-security repo?
TC: Issues are good for that.
AP: New discussion board/tab in Github?
MK: How do we enable this?
AP: Need to be enabled.
TC: Good idea
AP: Good for public Q&A. Let's just do an issue for now. **[Check with GA4GH re: Github discussion forum example Discussions · edgedb/edgedb · GitHub]**
TC: Passport clearinghouse definition/splitting should be an issue, but Work Order token is perhaps too big for an issue.
MB: Volunteers to create that issue?
TC: Tempted to. But resolving related issue of the intro & FAQ first - it might fall out of that. I can make an issue and then we'll see. I vote that we update the Intro and FAQ. Having an ADR as a more formal version of the ADR - I would be against that
AP: Yes, many of the decisions have already been made. Probably too late. I'll delete that branch and move the text to FAQ. Can we delete random documents in the repo? Random diagrams too.
TC: Are they not referenced somewhere?
MB: Hope we don't break some links!
TC: I will look into that. Maybe a PR. Not promising.
AP: Do we want the sequence diagrams into the FAQ?
TC: +1
MK: I like the flow of assertions to stay.
AP: No, the other diagram. Less important if it's in the FAQ.
TC: I'll copy them over.
AP: I'll delete my diagram branch after.
TC: There were two old do-not-merge branches. Reached out to David Bernick about removing it. Any objections? What about Craig's draft for 1.2?
KR: I don't think so. I'm not looking at it now. Most of what we discussed has been addressed.
TC: I'll comment and then close them.
MB: +1

Zoom Chat
00:05:22 Martin Kuba: https://github.com/ga4gh/data-security/pull/66
00:06:06 Max Barkley: https://github.com/ga4gh/data-security/pull/66
00:06:27 Martin Kuba: https://ga4gh.github.io/data-security/1.2-draft-passport-token-definition/aai-openid-connect-profile

00:13:11 Max Barkley: https://ga4gh.github.io/data-security/1.2-draft-passport-token-definition/aai-openid-connect-profile#conformance-for-passport-issuers
00:20:59 nstanar: Sry guys, I have to drop, have a dr's appt.
00:31:05 Kurt W. Rodarmer: Signed tokens provide very weak proof of client identity simply because there's no proof that the client is the same as the point of token origin.
00:35:56 Tom Conner: https://ga4gh.github.io/data-security/1.2-draft-64/aai-openid-connect-profile
00:36:41 Tom Conner: https://github.com/ga4gh/data-security/pull/67
00:49:10 Andrew Patterson: https://github.com/edgedb/edgedb/discussions
00:51:27 Kurt W. Rodarmer: Haha! Sorry.
00:51:38 Kurt W. Rodarmer: +1 Tom.

2022-05-26

Attendees - Name (Affiliation): Tom Conner (Broad)

Actions

	Actions Arising	Assigned To	Deadline
	Reach out to AP about sequence diagram	FL	
	Replace token type	MB	
	Draft new token type spec	MB	
	Cleanup links across the spec	TC	
	PR in Passports Spec	TC/MK?	

Agenda

	Agenda Item	Person/Time
1	Previously agreed changes: published branch and PR	
2	Passport Issuer as Broker function	
3	Need for SPA/PKCE support?	Carried over
4	New token type URN	
5		

Minutes

TC: Changes made as agreed previously. Claim Clearing House → Passport Clearing House. PR sent to Martin Kuba for approval.
https://ga4gh.github.io/data-security/1.2-draft-issue-62/aai-openid-connect-profile Others can give opinions. Sequence Diagram still needs to be changed.
TC: Clearing House is a Broker.

MB: Currently using generic JWT URN. Ideally a specific one, but will likely take too long to receive. Could use a te
MK: Make up a namespace for GA4GH and use it.
DB: +1

Current: <urn:ietf:params:oauth:token-type:jwt>
Suggested: <urn:ga4gh:params:oauth:token-type:passport>
MB: Submit as a new PR? Will do.
TC: +1
MB: need to define the token received for this URN. Previous discussion was around using a NIH v1.1 style JWT - signed token.
MK: Specify type of token in header - special value. The Committee for WS standardization (TASC) discussed new media type. *<application/vnd.ga4gh.passport+jwt>*
https://github.com/ga4gh/TASC/issues/36
MB: Will put together a draft spec for the new JWT type. This header, array of encoded visas.
MK: Custom visas are a type of visa.
MB: Avoid language forbidding anything, should be fine. Anything outstanding we need to modify?
TC: Cleanup links across the spec, not changing the meaning. Will hold until MB has completed Token type draft.
MB: These the only outstanding things before master merge?
CS: +1

FL: Clarification around AAI vs Passport spec versioning/changes.
TC: Passports will need to be changed to update references between the specs. So likely will see an increase in version number too.
MK: Should maybe make a PR in Passports Spec for this.
FL: Will include this language in the newsletter. What about mentioning work order tokens?
MB: Could plug the Work Order Token HACKathon session, but probably not much more than that.

TC: AAI Intro document needs revised.
MK: Needs changed, but perhaps wait until the final passes of AAI OIDC.

2022-05-19

Attendees - Name (Affiliation): Martin Kuba (ELIXIR-CZ), Tom Conner (Broad), Fabio Liberante (GA4GH), Kurt Rodarmer (NIH)

Apologies - Andrew Patterson

Actions

	Actions Arising	Assigned To	Deadline
1.	Make previously agreed changes (e.g. Claim Source -> Visa Assertion Source etc.)	TC	
2.	Cross-reference AAI and PP spec using ext links - issue	TC	
3.	Clarify Passport Issuer is a function of Broker (amend diagram to reflect this)	TC/AP	
4.	Table SPA/PKCE discussion for next meeting	FL	
5.	Table new token type URN discussion	FL	
6.	Prepare draft of approval flow for v1.2	FL	

Agenda

	Agenda Item	Person/Time
1.	Andrew Patterson Questions	All
2.	Martin Kuba Proposed Changes	All
3.	Next steps before merging into master?	
4.		

AP: Unfortunately I cannot be here tonight but have attempted a diagram for the Conformance for Passport Issuer section - I am not sure it sheds much light though. Possibly is better as a light weight sequence diagram.
https://ga4gh.github.io/data-security/1.2-draft-sequence-diagram/aai-openid-connect-profile

https://ga4gh.github.io/data-security/1.2-draft-sequence-diagram/aai-openid-connect-profile#conformance-for-passport-issuers

I do have some quick questions - that occurred as I was doing the diagram - perhaps could be discussed in my absence (or deferred to other meeting)

Conformance for Passport Issuers (s2)

In the case where a Passport Issuer is *not* the Broker, how would the client locate the Passport Issuer? At this point the client has a Passport-Scoped OAuth Access Token issued by the Broker - which is its only known (.well-known) endpoint. How would it know it should go elsewhere for token exchange and where would it go?

I think I'm unsure of where the requirement/use case for non-broker Passport Issuers is from - doesn't it have lots of implications throughout the spec? I.e Conformance for Claim Clearinghouses should be "Claim Clearing MUST trust as least one Passport Issuer" (as we have split off that role from Brokers)

Conformance for Passport Issuers (s4.2)

Surely this rules out any SPA apps (React etc) websites. These websites can do an OIDC auth code flow with PKCE - but they don't have a client secret and I'm not sure how they would meet the client authenticated requirement. I'm not saying the requirement is wrong - but we should have some guide how we'd do this as its an extremely popular modern web technique. Is there are PKCE equivalent flow for token exchange?

Martin Kuba proposed changes:

Remove double definitions like "Claim Source/Passport Visa Assertion Source" by moving definitions to AAI spec and referencing them from the Passport spec.

in AAI spec:

Claim Source -> Visa Assertion Source
Claim Repository -> Visa Assertion Repository
Claim Clearinghouse -> Passport Clearinghouse
in definition of Visa Issuer - replace "GA4GH Claims" with "Visa Assertions"
move definition of Visa from Passport Spec to AAI spec, not "A GA4GH Claim value or entry within a list or object of a GA4GH Claim that contains a JWT"

in Passport Spec:

Passport Bearer Token -> Passport-Scoped Access Token (reference to AAI spec)
Passport Visa -> Visa (reference to AAI spec)

Passport Visa Assertion Source -> Visa Assertion Source (reference to AAI spec)
Passport Visa Assertion Repository -> Visa Assertion Repository (reference to AAI spec)

Minutes

FL: AP was unable to join - discuss diagram.
MB: Diagram - possibly better as a lightweight sequence diagram.
KR: Broker and PP Issuer are not the same looking at the diagram?
MK: The text is also incorrect. An Issuer has to be a Broker.
MB: Combined into a single box?
TC: Can we provide multiple examples? Can a Issuer to use non-OIDC means?
MB: Would leave a hole that is incompletely explained? Implementations could deviate more.
TC: Broad?
MK: Token Exchange is defined for OAuth
KR: Our definition in particular does.
MB: Could still be a scenario with separate OAuth servers? No plans though.
FL: Is this a option
KR: If the Broker is only performing OAuth - then it's just an OIDC service.
MB: Trying to imagine a scenario where only one. My vote is that it doesn't make sense and should be the same thing.
MK: Must be the same thing.
MB: Passport Issuer is fine, but a function of the Broker
KR: +1 Pass Issu is the broker. Same thing
FL: 2020 Webinar
KR: Going back to far. No longer overloading the OIDC - Token Exchange. V1.2 adds this functionality.
MB: David Bernick - Token Issuer was an abstraction - but was translated into Passports. But names for different capabilities is good. Extensions to the Broker.
KR: +1. Function vs entities. One entity - but defining functions - and support for functions reflects version you are supporting.
MK: Sep definition of Passport broker.
TC: Can still use the definition less formally.
MB: Move Conf for Pass Issuer under Broker? Passport Issuing Broker.
KR: If it doesn't PP what does a Broker do?
MK: Visas
KR: Fair
MB: Keep a name for a bundle of features.
MK: A special type of Broker that could issue a Work Order
MB: When we add Work Order - add Work Order Issuer too?
TC: Keep Broker & Passport Issuer?
MB: +1
MK: +1
TC: Good test of new token type language. Why Broker?
KR: Source of Authority is not from the Passport provider. Much like DNS.

MK: 00:27:53 Martin Kuba: why broker -
https://ga4gh.github.io/data-security/1.2-draft-main/aai-introduction#why-brokers
KR: Uni may say researcher is good-standing, but not offer data or services. Problem is keeping track. Signed
FL: Care about tracking the original issuer?
KR: Original authority. Second hand claims are dubious legally and security-wise.

FL: What are the changes to make here? Does the diagram need to reflect what we discussed, or the text?
TC: Both.
MB: +1. Section 2 under Conformance for Passport Issuers. Passport Issuers must be Brokers. 2&2.1 need changed.
TC: Passport Issuer here was meant to be more generic initially. 2.1 - just strike. +1
FL: If you are issuing a Passport, you must have some degree of authority and are therefore a Broker.
MK: 2 - change Issuer is a Broker, as Broker is OIDC, it says everything.
FL: Issuer is a function of the Broker. Not separate entities, so it answers Andrew question of how can one not be both.
MB: Issuer is a Broker that meets all other requirements. Diagram needs to be updated to reflect this.
FL: Issuer within Broker box?
MK: +1
MB: +1
FL: Andrew's second question.
MB: Answered this as part of previous discussion.
MK: We should not say that a Claim Clearing house should trust at least one Passport Issuer. It may not trust any of them. Some Brokers may not be a Passport Issuer. Claim Clearing House must trust at least one Broker. That is correct.
FL: If the Issuer is not the Broker?
KR: MK can you expand on that? How is that a Clearing House would trust a Broker, that is not a Passport Issuer?
MK: If you are implementing a Broker v1.0 - it would issue the visas from UserInfo, but it is not Passport Issuer - as that is defined to issue Passports as JWTs.
KR: What we're really saying is that the Clearing House will be seeing Visas NOT Passports.
MK: Depends what Claim Clearing House is. Is it a Passport Clearing House? Do we want CCH that trust Visas, but not Passports?
KR: Anything that is a signed token, almost by definition you need to recognise and accept the signature. Or you should reject it. The reason Passport is signed, not because it contains info, just so it is a signed package. It will reject an entire Passport if signed by an entity it doesn't trust, but allow and skip over Visas it doesn't recognise as if they're not there.
MB: In v1.0 - CCH must trust at least one Broker - trust in so far as they believe that what they receive from the Broker UserInfo endpoint is accurate in representing the Visas for that user. It cannot forge Visas, but it can omit them.

KR: Because the visas are bearer tokens, it could also assign visas that do not belong to the user.
MB: True. Fair to say there is trust there.
TC: Can a Clearing House create a new Passport that combines Visas in a new way?
MK: Then it's a Broker. A chain of Brokers is possible. Clearing House only accepts.
TC: If you create a new Passport, even with the same Visas, then you're a Broker.
KR: Caution about going too far into the history of this spec. What was done initially, was not what we agreed upon in 1.0. Look to 1.0 onwards.
MK: Need to keep backward compatibility with 1.0.
KR: Don't argue with that. Just don't look backwards to older versions for language etc.
FL: Almost has a feel of legal language, of may, must and trust. Requirement of trust doesn't define what a client would accept, in terms of signed Visas, or signed Passports, it's just whether there is trust or not?
MK: Trust is not defined here.
KR: Implication of trust is not defined. What does that mean you have to do?
MB: My vote is not to change this section. Otherwise, be like OAuth and specify functional relationships.
FL: This language is unchanged from AAIv1.0.
MB: Anyone feel strongly we should change the trust language?
TC: Not me.
MB: Move on? AP's next point - client authentication is restrictive for single page apps? Proof Key for Code Exchange.
TC: PKCE is secure, but client is not in an SPA.
MK: Authentication is done by using the access token?
MB: In the token exchange you have a subject token, but you need to authenticate the client. Examples in spec are only using client id and secret, but technically you could use any OAuth mechanism. How would PKCE work for this?
MK: Just to make sure that an Attacker cannot steal the access code and exchange it for access token.
MB: Does it make sense to have SPA Passport Token support as a goal?
KR: Pros and Cons. RAS viewpoint - Passports being plaintext bearer tokens, should not be captured in browsers.
MB: DNAStack - usually keep those stored server-side and use cookies as token exchange. If no one on this call feels strongly, shall we table that for next week so Andrew Patterson can give his perspective?
KR: +1, but off next week. We are using SPAs, we have an approach, but different to what is described here. Eager not to put language into this spec around SPA support.
MB: absention. Anyone else?
FL: Let's table it, but could it be a discussion for v2.0?
MK: *Changes listed above.* Discussed previously. Move all definitions into AAI spec and reference them.
FL: Streamline the spec?
TC: +1. Will do that!
MK: Passport Visas = Visas

TC: Visa is not a reused word. External links more visible?
MB: Never been able to style the Markdown external links.
MK: Terminology section - list all External links - internal links to terminology section.
TC: Or square brackets like a bibliography. Small new PR - get it approved.

MB: Next steps before merging into master?
FL: GA4GH perspective or?
MB: Both - when will we feel ready to present?
TC: Feel like June.
MK: No further changes, then it will be fine.
TC: Level of controversy seems to be tailing off. Just tidying and merging.
MB: Is there a description of the Token you get back from Token Exchange?
MK: No. Reminds me that Conformance of Passport Issuers - says requested token type is JWT, but it should say that depending on this value it should issue different tokens. Maybe for PP - some specific string, but for a Work Order token type, the request will be something different.
KR: Wise +1
MB: Table this for the next meeting? A new URN for token type for v2.0 and a description of that token.
MK: Could be the same at what NIH already release, JWT with claim.
MB: Nothing needs to be fixed in this spec.
KR: Keep in mind - for v1.2 - it's not controversial what's in the PP, but we need a custom visa type.
MB, MK, TC: +1
MB: Not much to do overall then.
FL: GA4GH perspective. DURI Leads meeting - I will prepare a single page draft of steps between now and approval. Share with DURI Leads, then with this group and see from there.
MB: FASP Hackathon is coming up in June. What are Work Order Tokens? A session to sketch it out with the community. There is a lot of interest there.
KR: Plug - Work Order token is something we've been working on at dbGaP. Hopefully a working prototype for the September plenary. Something concrete to argue about in this meeting. I can already give a concrete description of what a work order token could contain. The functions are more important than the contents.
MB: Will make sure everyone is updated and co-ordinating with this

FL: Thanks everyone!

Chat log:
00:06:14 Fabio Liberante: https://ga4gh.github.io/data-security/1.2-draft-sequence-diagram/aai-openid-connect-profile
00:10:41 Kurt W. Rodarmer: @Fabio - can you post the link to the minutes? The link I see in the meeting invitation does not seem to be current.
00:12:54 Fabio Liberante: https://docs.google.com/document/d/14bHDgsv1rWSHRgHCxgkD39z_FXlHJrE08ENQDMUmGwY/edit
00:13:01 Fabio Liberante: Apologies Kurt
00:20:57 Kurt W. Rodarmer: +1 Max - we are making more concrete names rather than using abstract functional names.
00:27:53 Martin Kuba: why broker - https://ga4gh.github.io/data-security/1.2-draft-main/aai-introduction#why-brokers
00:51:36 Kurt W. Rodarmer: I don't want simple bearer tokens in the browser. The WorkOrder token is intended to be provided to users for administration.
00:59:09 Kurt W. Rodarmer: Keep in mind that for post-authorization cases like NIH, we need a custom visa type.

2022-05-12

Attendees - Name (Affiliation): Tom Conner (Broad), Martin Kuba (ELIXIR-CZ), Andrew Patterson (UMCCR), Max Barkley (DNAstack), Michele Mattioni (Seven Bridges), Kurt Rodarmer (NIH)

	Actions Arising	Assigned To	Deadline
1.	Diagram for “Conformance for Passport Issuers”	AP	
2.	Merge Token Exchange with 1.2-draft-main (with approval)	TC	
3.			
4.			

	Agenda Item	Person/Time
1.	Review https://github.com/ga4gh/data-security/pull/56	All
2.	Discuss merging to **1.2-draft-main**	All
3.		
4.		

Summary Current status of Passports v1.2
Passports/AAI Use cases from 2021 v1

We discussed in our 2022-02-17 meeting having three steps to getting to 1.2:

1. *the use cases and introductory explanations*
2. *the token exchange details*
3. *modifying the DURI spec minimally as needed to describe necessary changes to claims, visas, and passport.*

The updated branch is published at
https://ga4gh.github.io/data-security/1.2-draft-token-exchange/aai-openid-connect-profile

PR Review:

- Discussion around referencing previous Visa definition from a particular version, or tag/release.
    - https://github.com/ga4gh/data-security/pull/56#discussion_r870802124
    - Jekyll in the future to make approved spec publishable/available?

- Cite OIDC userinfo & token endpoints directly to avoid confusion
    - https://github.com/ga4gh/data-security/pull/56#discussion_r871267236

- Remove “public-facing” for userinfo endpoint
    - https://github.com/ga4gh/data-security/pull/56#discussion_r870814465

- Broker **MAY** support Token Exchange - allows compatibility.
- MB: Do we need multiple Visa Issuers in this release? MK & AP: No.
- Can we deprecate/ strongly recommend not to use/implement this section?
    - https://github.com/ga4gh/data-security/pull/56#discussion_r871319525
    -
- ML:
- KR:

- MB: Non-prescriptive flow diagram for “Conformance for Passport Issuers”?
- AP: Happy to try it.
- TC: Merge this PR first and then the diagram afterwards. AP: +1
-
- TC:

2022-05-05:

Attendees - Name (Affiliation): Tom Conner (Broad), Kurt Rodarmer, Max Barkley, Fabio Liberante (GA4GH), Alice Mann (WSI), Martin Kuba, Michele Mattioni, Mikael Linden
Apologies: Andrew Patterson (University of Out with Covid)

	Actions Arising	Assigned To	Deadline
1	Make agreed changes to <Token exchange details for 1.2> branch and distribute for approval	TC	Next meeting
2			
3.			
4.			

	Agenda Item	Person/Time
1.		
2.		
3.		
4.		

Summary Current status of Passports v1.2

Passports/AAI Use cases from 2021 v1

https://github.com/ga4gh/data-security/pull/55
We discussed in our 2023-02-17 meeting having three steps to getting to 1.2:

4. *the use cases and introductory explanations*
5. *the token exchange details*
6. *modifying the DURI spec minimally as needed to describe necessary changes to claims, visas, and passport.*

MK: Why double signature?
KR: Short and profound answer. Visa must be signed, but signing the whole Passport aids authentication. The
KR: The visa alone does not provide authentication. Broker an decides this. Broken chain of authority. Visas could be handed out to anyone
MK: Separation of Broker and Visa Issuer is the vulnerability that needs to be addressed?
KR: Yes. Requires recognition of Visa Issuer, which may not always be the case.

AM: Question raised at Connect meeting about NIH approval
KR: Presenting internally at NIH tomorrow. Should have final decision on v1.2 shortly thereafter.

MK:
KR: Likely GA4GH hit 1.2 before RAS implements. Dependency on Passports/AAI work order token to allow implementation at NIH with RAS project.

MB: Discussed at FASP meeting - perhaps a summer hackathon to test out v1.2. Is that premature to demo a work order token?
TC: Close to approving 1.2, think May is possible.
KR: Close to working prototype for work order token. Produce an NIH reference version.
MB:

TC: 1.2 token exchange branch changes. AP not on call, but contributed heavily to this. Propose going through that branch now.

KR: Issue with “authentication” in new 1.2 Abstract. Token should not be used for authentication. Exchange means that original user could be anywhere.
“`authentication and authorization purposes by downstream`”
MK: The content of the claim (a token) is for authorization, not the groups of claims as a JWT.

TC: Explicitly mention how AAI are used with Passports in less ambiguous terms.

MB: Introduce concept of Visa before the claims they are

KR:

TC: Claim Source becomes Visa Source
ALL:+1

KR: Embedded Tokens terminology covers non-Visa uses.
TC: Only using Visas for now.
KR: Precedent for changing definition later in JWT Spec, e.g. string>string/URI
ALL: +1 for replacing Embedded Token with Visa

Diff for <Token exchange details for 1.2> https://github.com/ga4gh/data-security/pull/56/files

2022-04-14:

Attendees - Name (Affiliation): Tom Conner (Broad), Kurt Rodarmer, (NIH), Heidi Sophia (NIH), Max Barkley (DNAStack), Alice Mann (Wellcome Sanger Institute), Mikael Linden (ELIXIR-CSC), Christoph Zwerschke (GHGA)
Apologies: Martin Kuba, David Bernick (Broad)

	Actions Arising	Assigned To	Deadline
1			
2			
3.			
4.			

	Agenda Item	Person/Time
1.		
2.		
3.		
4.		

Minutes

- Connect: Kurt and Tom can make the FASP session to represent Passports
- Backing off being overly prescriptive of the technique for how revocation happens. Spec has detailed rules that pertain to one use case and not applicable to all use cases.
- Idea to say you have to have a revocation mechanism and leave the specific descriptive details out.
- Tom has a PR on that

2022-04-07:

Attendees - Name (Affiliation): Tom Conner (Broad), David Bernick (Broad), Kurt Rodarmer, (NIH), Heidi Sophia (NIH)
Regrets: Alice Mann, Max Barkley

	Actions Arising	Assigned To	Deadline
1	Create PR to change “data owner” to “data controller” and mention that data controller is the source of original authority.	Tom	14 April
2	Create PR to change access polling and other revocation implementation details	Tom	14 April
3.			
4.			

	Agenda Item	Person/Time
1.	Tommi Nyrönen suggests a terminology change: • One term "data owner" strikes my attention. Could also be named to be equivalent to "data controller" to increase interoperability with EU gdpr. • "Data holder" is a recognised term in the forthcoming Data Governance Act that is expected to improve data sharing in the EU.	
2.	Revocation changes	
3.		
4.		

Minutes
Discussed “data owner” change. Kurt observes authority is another word that could be used. Tom will take an action to make a PR to give an opportunity for others to comment before. “Data controller is the source of original authority” .

Regarding revocation. Kurt: RAS team took to heart the polling requirements in the spec. Would like to change it in both RAS and GA4GH. Visa authorizations can’t be used if older than an hour. Authzns should be checked for revocation. We also should specify behavior if unable to check for some reason.

2022-03-31:

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation):, Tom Conner (Broad), Max Barkley (DNAstack), Kersten Breuer (GHGA), Christoph Zwerschke (GHGA), Michele Mattioni (Seven Bridges), Martin Kuba (ELIXIR-CZ), Moritz Hahn (GHGA), Heidi Sofia (NIH), later: David Bernick (Broad)

	Actions Arising	Assigned To	Deadline
1	Andrew - adding section below non-normative to explain link to Passports spec from this AAI v1.2 spec	Andrew patterson	
2	Check in with Kurt, David and at Broad to make sure ok with minor change on revocation, not say must and enumerate a couple of different options, maybe do a minor branch	Tom Conner	
3.			
4.			

	Agenda Item	Person/Time

1.	Carry on from last week:
	Previous Spec action items:
	- Move to informational section
	  - Claim Management System
	  - Claim Repository (this one is referenced, but references could be reworded)
	- Leaving in (talked about moving)
	  - Claim Source: confirmed leaving in the terminology section.
	- Discuss revocation in next call as it relates to different kinds of tokens
	- Possible differences between passport tokens and visa tokens	

2.		
3.		
4.		

Minutes

Previous Spec action items:

- Move to informational section

    - Claim Management System
    - Claim Repository (this one is referenced, but references could be reworded)
- Leaving in (talked about moving)
    - Claim Source: confirmed leaving in the terminology section.
- Discuss revocation in next call as it relates to different kinds of tokens
    - Possible differences between passport tokens and visa tokens

- AP: re did the diagram and moved to informational section, that is all on a branch and I tagged everyone in the branch for review. Happy to merge it when we have agreement
- I made the concept of claims generic and abstract
- Andrew sharing the link: https://ga4gh.github.io/data-security/1.2-draft-flow-of-claims/aai-openid-connect-profile
- Pull request bit: https://github.com/ga4gh/data-security/pull/58
- MB: diagram looks great
- AP: ability to be edited on the fly in the spec hopefully outweighs it looking particularly fancy
- Are we putting the rationale in the spec? We need to come up with some common formatting
- MB: talked about wanting to have non-normative examples for how v1.2 ought to be used. Section on non normative diagrams and examples
- TC: fine without the blue box
- Like setting the stage for introductory information
- TC: the data and how you reference the data and identifying with DRS IDs, whatever particular ways that datasets are identified, should that be represented in a different diagram.
- AP: sequence diagrams, could fill in in detail at end or a separate diagram showing less of sequences and more of flow of interactions/nodes. Sequence diagram doesn't show you looking like with lots of DRS servers and IDs.
- TC: I wouldn't clutter this diagram
- TC: I think we should merge it
- MB and TC approve so AP will merge that branch
- AP will email when he does stuff on github as the notification systems seem unreliable
- CZ: why called claim repository and different in the spec?
- AP: good question, some distinction will be intention, some concept of this spec having some abstract concepts and passport spec have specific things, so DURI did some naming i think. We have since decided that was confusing everyone so maybe we should
- MB: i don't think we changed any of the names of anything in the terminology section, it refers to specifically a claim clearinghouse, i think same concept but in the body of spec it might call it a passport clearinghouse even though claim CH in the terminology section. Passports only current usage of AAI, part of v2.0 we will move AAI and passports together to remove potentially unnecessary distinctions
  ML: v1.0 originally introduced visa concept, didn't want to use the word claim as it's a

reserved word for people familiar with OIDC, do we need to take that into account here as well.
- CZ: passports spec also contains the word claim, passport claim.
- MK: same claim but AAI spec says they are GA4GH claims in abstract and there is only one type of claim and that is the passport claim. We can define other claims but no other claim was define.
- CZ: clarify passport claim could be an implementation of AAI spec.
- AP: which direction? AAI not meant to mention passports but can't edit passports spec at the moment. For v1.2 just try to tidy up language if we could but not rename any of the definitions.
- MB: if non-normative section for other things, right below for flow of claims make sense of relationship to Passport. Doesn't need to be part of the spec, but description that intent of this document to be used with passports, passport claim is..
- AP: take as action item.

Discuss revocation in next call as it relates to different kinds of tokens
- Possible differences between passport tokens and visa tokens
- https://github.com/ga4gh/data-security/blob/master/AAI/AAIConnectProfile.md#token-revocation
- Need Kurt's comments on this really, next week?
- No mechanism to revoke individual visas at the moment, revoke the passport
- MK: passport life short, one hour. Different visas different times depending on the type. Affiliation to organisation is for one year. Some are shorter i think. It was always a problem, nobody wanted to specify for how long something was valid.
- AP: no individual revocation for individual visas
- MK: implementation of the broker, someone asks userinfo loads fresh visas from the sources.
- KB: mechanism used for long-lived access tokens and short lived visas. Remove visa from claims repository and after an hour find out- CSC implementation as the CH
- ML: that's correct.
- TC: doing every one hour coming and checking if the visa is still valid.
- AP: only where the passport is still valid. Refetching fresh passport, not revoking visas
- TC: done as a choice to honor revocation?if long running job doesn't seem like a core requirement that it would need to check for permission.
- KB: use case in CSC remote desktop environment, users have continuous access to jupyter notebook e.g with data and ensure user has continued permissions to access their data.
- TC: okay so here naturally need to keep getting access though passport could be cached in their system
- MB: might be worth documenting as non-normative way as one option you can use/ in passport spec we have what you need to validate a visa? If expired not valid. Out of spec you may be confused if see that, if get a passport and visa expired is it worth checking again if have new visas. In some systems yes, in general maybe not. Do we

want to document that? You can have changing claims or just leave it as a use case that we can document in a non-normative way.
- ML: job for 20 days say, freshness of revocation of visas checked every hour, what if network hiccup in 20 days and checking revocation fails then need to terminate job.
- TC: what are the privacy and regulatory requirements around terminating access?
- KB: do we need to specify in the visa or passport token, whether issuing party expects you to check for revocation. If we at GHGA consuming for visas from NIH and NIH has strong revocation mechanism in place, long-running visas but are relying on revocation continually checked. Then might want to indicate in their visas, long-lived but might want to check once a day at least if visa token still valid.

Did we get through all of the terminology section?
- Bearer token?
- Can exchange for a passport
- MK: Passport scope doesnt mean its a JWT and contain scoped claim, could be an opaque value
- One of the scopes is a passport
- AP: in spec must be a JWT in a particular format, use of opaque token?
- MK: historical reasons I think
- AP: one of node JS (reference implementation of OIDC)) I was trying won't issue JWT access token, requirement in passport spec is that they were JWTs, necessary any more? Maybe not for v1.2 discussion
- ML: CH may accept access tokens so need JWT.
- AP: but TE immediately after flow, no longer necessary to be JWT in this case, can be any token
- ML: if client has several brokers? How does downstream.
- If first one still confusing, if access token sent in API in downstream server may be confused.
- Stuck with supporting JWTs.

Visa issuer
Visa

Terms I think we are ok with those as they are?

Next time
- Hope to have revocation issue settled, branch by next week?
- Visa definition (originally embedded token) definition does not specify it is a visa, can be any token. Should mention contains special claim ga4gh visa
- DB: good idea.

FASP passport sessions
- DRS and/or discovery
- April 22nd 10:00 Eastern

- Willing and able to attend?

2022-03-17:

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation):, Martin Kuba (ELIXIR-CZ), Tom Conner (Broad), Kurt Rodarmer (NIH), Michele Mattioni, (Seven Bridges), Andrew Patterson (UMCCR), Max Barkley (DNAstack), Mikael Linden (ELIXIR - CSC), Tommi Nyronen (ELIXIR - CSC), Kersten Breuer (GHGA), David Bernick (Broad); VIvian OTA WANG (ODSS-NIH)

	Actions Arising	Assigned To	Deadline
1			
2			
3.			
4.			

	Agenda Item	Person/Time
1.	If MK present: GA4GH namespace - update from TASC	
2.	Broker discussion if full group present	
3.		
4.		

Current abstract (with my edits already in place):

> This specification profiles the OpenID Connect protocol (OIDC) to provide a federated (multilateral) authentication and authorization infrastructure for greater interoperability between genomics institutions in a manner specifically applicable to (but not limited to) the sharing of restricted datasets.
> In particular, this specification profiles tokens, endpoints and flows that enable an OIDC provider (called a Broker) to provide GA4GH Claims to downstream claim consumers (called a Claim Clearinghouse).
> **DO WE WANT A SENTENCE HERE BASICALLY SAYING - “These claims can be obtained by a callback from Clearing House to the Broker or through token exchange by client with the Broker”**

The GA4GH Claims, nominally a GA4GH DURI Passport, can then be used for authentication and authorization purposes by downstream systems.
This specification is suggested to be used together with others that specify the syntax and semantics of the GA4GH Claims exchanged.

Minutes

- MK: update on media type `application/vnd.ga4gh.passport+jwt` something like that
- https://github.com/ga4gh/TASC/issues/36#issuecomment-1062720259
- Agreement on MK's suggestions

- MK questions: why is the aai token endpoint mentioned? TE specifically says the TE should be used so why is it introducing a new endpoint
- TC: yes I was confused, i will fix that
- We brought back references to the userinfo which is not being used entirely
- What is the difference between embedded token and visa? And embedded token issuer and visa issuer, is it the same so why two terms?
- KR: aai original idea is to be abstract and DURI concrete, since AAI really only has one example of anything concrete effectively the same but envisioned to be something else. Could have a different type of token that didn't carry visas
- MK: do we want aai to still be abstract? It looks confusing
- KR: i agree with you on that MK, if we were to categorise that one side is token techn and other side is vocab for expressing some other issues that is what DURI originally intended to express. Reason for separation is that, then DURI took over majority of token tech stuff. Yes not be so abstract
- MB: should we do that after v1.2? Or augment definition of embedded token in v1.2 to make it clear that this is meant to be a general term but only specific instance of this that spec deals with is a visa?
- KR: if something like a forward reference I don't think that would be damaging.
- TC: want v1.2 to land and quickly and be as minimal as possible. We have already said we were going to merge this stuff.
- MB: does that translate to leave definition alone?
- DB: we should be very visa focused right now. Questions we get the most are that kind of stuff, not the future kind of thing. I think we should focus on the visa.
- AP: visa issuer, visa aka embedded token and down in visa section, we introduce visa access token and visa document token neither defined in definition section, which is confusing.
- TC: a visa can be an access token but that may not be what the definition would say
- We don't have the two different types of visa in definitions.
- AP: in my head all visas self contained, but spec says visa access token, thing in visa is not the claims, call to visa issuer rto get the claims

- KR: we dont use indirect or introspection approach at NIH, our visas are fully fleshed out. Main thing is a token that can be resolved if already self contained ready to go if not go through upheaval of retrieving it, with more points of failure
- AP: adds bit of complexity into implementation and spec, non-obvious way it works. Needs to be in sequence diagram or long hard thing about whether we actually want to. Indirect visas don't make sense. I'd flag this as unless we can find users that are using it.
- KR: produce fully fleshed visas right from get go, upper limit from the engineering standpoint, tokens could be too large to pass. Kicked can down the road hoping v1.2 would fix it.
- ML: i believe the use scenario , several brokers in chain, downstream broker can place upstream access token to upstream broker, using userinfo endpoint for visas
- DB: yes but being used or should we keep it?
- AP: can keep it but need to flesh out definitions to make sure it's clear
- MB: not get rid of it but not allow it in self contained passport format. For that format, the visas have to be visa document tokens.
- TC: visas are document tokens.
- What exact term do we want to add?
- AP: visa access token and visa document token along with visa and visa issuer

- MB: last time trying to work out way to the PR.
- https://ga4gh.github.io/data-security/1.2-draft-token-exchange/aai-openid-connect-profile

Starting from beginning
- All happy with IDP,
- Broker: chain of brokers, brokers may also be claim clearinghouses, have we actually seen that in implementation? We don't know what ELIXIR is doing there. Theoretical chain of brokers
- Ok leave chain of brokers in the definition
- MK: claim repository can be different from claim source, claim management system (CMS) could get rid of but in ELIXIR you have some source which is an organisation then a claim management system where it is written.
- AP: not specified in spec as to how any of this worked
- MK: not necessarily to have in spec as spec makes no use of it
- KR: not actually specified it is just mentioned
- CMS was in previous version, forward references to claim source and claim repositories.
- We did suggest getting rid of the CMS or move to informational section not part of the actual spec but as an addendum.
- AP: i may do that to see what it looks like. Non normative here is some info about how we think claims might work
- May re-render that diagram as to plant URL diagram. In markdown so not needed as separate image.
- TC: or use mermaid
- KR: make sure that we give a little more form to the discussion around Clearing house and suggest that we re visit the token polling mechanism for revocation. That ended up

being something that was made to work but it might be time to look at it again and make sure it still makes sense

- KR: NIH passport curenyl contains dbGAP visa, dbGAP DRS only concerned with dbGAP visa even if others in play, dbGAP DRS calls the dbGAP CH only concerned with dbGAP and we are not in a position of needing to calling back to another section of NIH if token has been revoked as we are dbGAP, can check at resource server. RS employs whatever mechanism it needs to enforce it. In order to conform with GA4GH firewall to call out to another section of GA4GH that we have told them something has been revoked.
- DB: models TLS for revocation, we needed to find a revocation mechanism as this stuff is so asynchronous. This is what we came up, any improvements or clarifications welcome
- KR: think it was the best approach available with what we had to work with at the time, as we move forward, clarifying use cases, it might be good to question those initial assumptions gain
- DB: don't want to take out revocation.
- KR: requirement is to support revocation but technique we need to look at.
- MK: oauth already has mechanism for checking revocation of access tokens, can't we just re use it?
- KR: it doesn't work
- MB: which tokens?
- AP: both i think this is referring to. I think spec is talking about both passport scoped access tokens and visa access tokens (for revocation)
- KR: generate a token with long life time.
- MB: in tying it back to what in the spec this would relate to, in NIH case relating to the 1.1 JWT that we use.
- KR: client doesnt do the work, client sets up work, client passes token downstream, this can last a month or more for genomics. Downstream process encounters timeout but can't refresh, so oauth revocation mechanism not applicable. Broker model, uni auth issuing visas but broker takes care of that but visa issuer issues longer lasting token.
- MB: passport access token use to get visa from userinfo in v1.0 spec that is an oauth access token as get it from OIDC flow, so i don't get which token that isn;t a visa we need a special mechanism to revoke?
- Kersten Breuer: long running jobs, specifically when talking about processing of genomic data, how we have been thinking about it at GHGA (German human genome-phenome archive) that we only need authorisation once the workflow run starts, then workflow management system will pull the raw data into the infrastructure where it is operating on, this has to be authorised and then the processing as you mentioned can take a long time, more than a day often. That is not necessarily something where we need additional authorisation usually our use cases is self contained job that has started, it's running, no need to get any additional data, once it is finished result is deposited somewhere when we talk about genomic analysis as a user comes selects some data where user has controlled access to, workflow to run on that data, then the only occasion where we need authorisation apart from starting workflow is when user tries to retrieve result of the

workflow. This is how we avoid this long running jobs in case of genomic analysis. It covers our use case.

- KR: unlikely to fit NIH model, revocation to revoke it after already been granted. OAuth model much more instantaneous model
- Kersten: is really afraid that in the meantime of processing something is revoked and stopped processing no legal ground anymore then that's a different model.
- KR: short lived tokens around human speed, need for revocation of tokens go away
- MB: add action item to discuss something next meeting
    - Discuss clarifying revocation as it relates to different kinds of tokens.
    - distinction between different token types

Spec action items:

- Move to informational section
    - Claim Management System
    - Claim Repository (this one is referenced, but references could be reworded)
- Leaving in (talked about moving)
    - Claim Source
- Discuss revocation in next call as it relates to different kinds of tokens
    - Possible differences between passport tokens and visa tokens

2022-03-10:

Chair:
Attendees - Name (Affiliation): Max Barkley (DNAstack), Tom Conner (Broad), Kurt Rodarmer (NIH), Andrew Patterson (UMCCR), Nicole Bolliger (Broad), Jim Basney (CILogon), Alice Mann (GA4GH)

- https://ga4gh.github.io/data-security/1.2-draft-token-exchange/aai-openid-connect-profile
- GA4GH claims phrase needs to be clarified
- Is aai token exchange is the token endpoint we are adding.
- Yes MB suggest looking at what it is called in the OAuth spec, is it just OAuth token endpoint?
- TC will reconcile that
- AP: OIDC: the client and only the client, access token given to original OIDC token and passport scoped access token never leaves the client, downstream things yes do we need to clarify claim clearinghouse. They don't call back to get things
- KR: clearinghouse will have a different meaning depending on whether it is the authorising entity, authority that looks at ELIXIR user attributes and renders an authorisation than it is a different beast to NIH where authorisation taken place days or months before and CH is enforcing that the access has been pre-authorised.
- Both called CH, everything v1.0 all geared toward ELIXIR model so may be appropriate for ELIXIR model but not way NIH uses CH.
- AP: agree but name of entity that does TE is clear, TE done by the client
- KR: agree, clear to any person understanding OAuth terminology
- AP: keep user info bits on spec different to TE, who can do TE is restricted and as different to who is hitting userinfo endpoint
- KR: yes very good
- TC: client that does TE itself and CH flipped to sequence diagram branch, CH one of two columns on data holder
- AP: literal data may not be held by CH. CH that need to call back and keep user info will behave different to CH that consume JWTs, should we call them different CH or different words entirely?
- KR: not sure how everyone at NIH feels, need authorisation to introduce new terminology
- MB: could have more specific sub definitions?
- KR: may be all that is needed, leave claim CH as what has been since v1.0, introduce another term
- MB: first usage of CH usage in the PR markdown?
- TC: first instance right in abstract at the top
- AP: add two sentences in the abstract, there's a broker, either allow DS access to consumers with userinfo or TE to get a thing that is then used downstream. I will make changes directly on the branch

- Good with abstract for now

Terminology

- GA4GH Claim - sort of correct can be mean passport or visa. Do we need to address this?
- MB, AP agree fine
- KR: version built into claim name
- MB: will it need to change for v1.2?
- AP: changing name of claim big deal for backwards compatibility, maybe needs to happen in v2.0, no breaking changes here so claim names will just have to stay the same
- Claim management system:
- Claim repository:
- AP: we don't specify at all where the claims go, do we talk about this terminology at all?
- KR: CMS i think is out of spec. Nothing that ga4gh is defining about a CMS
- KR and TC suggest we get rid of CMS
- MB: agreed if no dependency on that terminology then that's a positive change
- Claim repository needed for implementation but undefined by GA4GH, out of scope in this spec. Mentioned in 7 places. Claim repository is in flow of claims so may need new terms. Is this describing GA4GH spec? **Tom will take an action to investigate this**
- AP: can we move this to an informational section?
- Claim source: referring to source claim inside visa JWTs?
- KR: might be more generic but refers to visa issuer or original authority
- MB: assume that needs to stay?
- Ap: do we have a thing for visa issuer? Linked to visa issuer to make it clear?
- MB: in visas there is an issuer and a source. Might mean something specific. Issuer in JWT sense signed the visa and source logical concept. Signer could be different to who they claim to be signing for.
- KR: exactly why the ambiguity was introduced.
- TC: Broker i dont think causes confusion?
- MB: do we need a change to allow for the fact that can do a TE as not part of OIDC.
- KR: yes agree …
- TC: not saying OIDC provider anymore
- MB: yes saying its a service that has APIs x and y, OIDC and OAuth TE, as Kurt suggested.
- KR: broker introduced to solve a problem that may be addressed with other things we are doing. Needs to stay right now but start to minimise it's utility over time that is a benefit
- AP: **pin in it to re visit second part of sentence when we have ELIXIR folk and David Bernick on the call**
- KR: we should tackle the CH definition more concretely.
- TC: focus on that and sequence diagrams next meeting

- MB: reviewing hackathon outcomes, we had a session led by Jeremy discussing test cases that can become part of a GA4GH test suite to become part of DRS and passports and a test suite for implementation compliance testing.
- What's a good next step? Are we not ready to do anything here? What is a milestone for when is a good point to bring it up with Jeremy again?
- MB: operational issues to the testing that will need to be addressed. Don't think we are ready yet but when we have the sequence diagrams refined based on the new spec that would be a good time to pick up that conversation with Jeremy
- MB: take action item to give update to FASP that still working on the diagrams

Notes
TC: Done a bit of work in the token exchange PR. proposal: dig into the PR
MB: Want to add to agenda: follow up on a topic that came up in FASP; want to talk follow-up on hackathon topic on testing of DRS-passport integration – possible next steps
TC: Review the diff or the raw file?
MB: Maybe walk through the files. Diff is hard to read.
TC: Files link: https://github.com/ga4gh/data-security/pull/56/files
TC: Last time I had made changes that were that removed all references to userinfo. That was a bit radical so that's been backed out.
MB: Question: so what would be returned from the userinfo?
TC: It would return the users information alongside the ga4gh visa claims as defined in the 1.0 spec. The new endpoint separates that so we're not intermingling the user information and the visas.

2022-03-03:

Chair:
Attendees - Name (Affiliation): Max Barkley (DNAstack), Tom Conner (Broad), Scott Koranda (CILogon), Kersten Breuer (GHGA, ELIXIR DE), Kurt Rodarmer (NIH),
Martin Kuba (ELIXIR-CZ), David Bernick (Broad), Michele Mattioni (Seven Bridges)
Apologies: Andrew Patterson (UMCCR)

I have made some updates to the sequence diagrams - apologies I can't make it to the meeting tonight (andrew). Leave any actions as comments in the PR and I can edit tomorrow.

Minutes
TC: Call for Agenda
MK: Last time we ended with whether we want the new token to be in the same format as NIH uses or something else
TC: Do we want to do that?
MK: Sounds good
MB: Should we move forward with that or do we need to look at it on this call?
MK: Might be worth looking at claims in the token?
KR: Seems like what we've just said is significant enough to be own milestone; let's record that and work out the details later

Walking through NIH token: https://auth.nih.gov/docs/RAS/serviceofferings.html#AppendixA

TC: So we're looking at the "RAS Passport Decoded with Encoded Visa"
KR: Passport token more or less has all the same content as the user info but encoded as a JWT.
KB: New to this meeting; can someone help me get up to speed
KR: Token has some NIH specific claims I can explain if needed. "Sub" is an anonymous user ID. scopes have been reduced to "openid ga4gh_passport_v1" to remove "profile email" scopes that would have extra user information. "Txn" is for associating multiple tokens with each other
KB: How do you get this passport token?
KR: You get it from user info with the access token from OIDC.
MB: Anything else to discuss?
TC: The visa looks like it's NIH specific
KR: This is a custom visa, but this would work with regular visas, but we should keep the escape valve for custom visas. We can't put all the content in a visa because it has a custom vocabulary
MK: Why does the visa contain the scope claim?
KR: The spec says that any GA4GH JWT must contain scope claim, but it serves no purpose
DB: We can change that if necessary
KR: Our clearing house mandates its there, but we don't use it, just to be spec compliant
DB: Once we move to a place where access tokens aren't being passed downstream, and user info is just user info, then maybe we don't need this
MB: Is "txn" a standard claim?

KR: No. If there is a standard three-letter claim for that we'd be fine with using, but this is important. We include the txn in URLs and it shows up in access logs
MB: Makes sense. I think we probably don't want to mandate "txn", but allow for extensions
KR, DB: The intention of the original passport was to allow for extension
TC: <Question about txn>
KR: Literally every token has its own JTI, but every token that is generated off the same authentication event has the same "txn"
MB: Seems like we have rough consensus, so maybe discuss next steps?
TC: I can try to incorporate this into the spec, but I will need comments
MB: So the recipe for 1.2 is adding new diagrams with context, token exchange endpoint, token format and how to get it with token exchange?
TC, MK, KR: General agreement
TC: Do we want any changes to how user info works in 1.0?
DB, MK: No keep it for backwards compatibility
MK: There are two types: requested_token_type (URN) for token exchange, and media type in JWT header; they have to be different
MB: There will probably be input from other conversation on GA4GH IANA namespace, but we should decide on the "right-hand side" of that URN that is the conceptual name of this token. I recall someone was partial to using "passport" in name in our last meeting?
TC: Can't just be passport; that word is overloaded
DB: Maybe nothing should be the passport and passport is the name of the whole system
MB: How about "self-contained-passport-jwt" as name?
DB: Yes, I may have proposed that name in my PR before
General agreement
MB: So start new PR or same PR?
TC: Same PR: https://github.com/ga4gh/data-security/pull/56
TC: This PR is into "1.2-draft-main" branch, where we'll work on all 1.2 changes until we're ready to merge that into master
TC: This is the PR for 1.2-draft-main: https://github.com/ga4gh/data-security/pull/55; PR has links to other branches as well
TC: Using DB's old branch for some of the language around token exchange
TC: Speaking of old branches, there are some old, inactive branches that we might want to get rid of. There was a "1.2 minor changes" that has been merged. "1.2 craig inactive" that seems like we don't need those.
TC: Will send an email to group with branches that I will delete before I do it so people can object.
TC: There's another PR Andrew opened that I don't want to kill, but maybe we should discuss it in the future (when Andrew's here)

From chat: KB: I like the "self-contained-passport-jwt" but just to add another naming option, what would you think of "passport aggregate"? It is a bit less descriptive than "self-contained-passport-jwt" but it's more concise and more consistent with the other GA4GH vocabulary such as "passport visa" or "passport claim".

MM: There is a DRS PR about how to get a passport token that we might want to look at: https://github.com/ga4gh/data-repository-service-schemas/pull/381
TC: Yes this PR has come up before.
MM: Problem is that we have many DRS servers and there isn't one way to authenticate for all objects across all servers
MB: Maybe we should think about how we want to tackle this operationally? Should we iron out details of AAI/Passport 1.2 first?
General agreement

Action Items:

- TC: Update PR with language around token based on NIH RAS 1.1 token
- Everyone: Review that after Tom emails AAI group

2022-02-24:

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation): Doug Voet (Broad), Martin Kuba (ELIXIR-CZ), Tom Conner (Broad), Heidi Sofia (NIH), Max Barkley (DNAstack), Andrew Patterson (UMCCR), Nicole Bolliger (Broad), Vivian OTA WANG, Scott Koranda, David Bernick (Broad), Kurt Rodarmer (NIH)

	Actions Arising	Assigned To	Deadline
1	AP: changes to sequence diagram as discussed	Andrew Patterson	
2	MK: wil take a look at the flow that is currently supposed to be representing the ELIXIR implementation	Martin Kuba	
3.			
4.			

	Agenda Item	Person/Time
1.	Action review GA4GH namespace - going to be discussed at TASC Connect workshop - in planning	
2.		
3.		
4.		

Minutes:

https://github.com/ga4gh/TASC/issues/36

- AP: document visas or access token visas in the spec, AT visas are thing that gets embedded into passport is another access token to be called back to the broker to get the content of the visa.
- DV: RAS does use those, however they do contain the content but you need to validate it hourly.
- AP: i thought it was an opaque token and you had to go fetch it.

- DV: main issue is revocation, access token you can revoke it but with the document visa there is no revocation mechanism
- AP: worth showing those in the sequence diagram. I will put both of those sequences into the sequence diagram
- TC: let's make this sequence diagram the main focus on this.
- DV: what was written in the existing version of the spec for this access token visa, is not how the NIH did it. Probably stems from the fact that their visas are too big to be headers, potentially. That's something to keep in mind in thinking about this works in the next version of the spec.
- AP: good to tease out how we are documenting that, is there a convergence on some way that everyone can do it the same as NIH.
- AP: i split into two and apologies in the sequence diagram. Two major flows currently in use,. I called it ELIXIR callback flow and the new token exchange flow.
- Going through the sequence diagrams now: https://ga4gh.github.io/data-security/1.2-draft-sequence-diagram/aai-openid-connect-profile#appendix---sequence-diagrams
- Official OAuth specification has come out now october last year, OAuth access official token names, spec says what JWT access token would look like. Call them an OAuth access token. I called the thing that you get from the initial OIDC flow is the passport scoped OAuth access token. We need to distinguish between lots of things now.
- TC: sounds good. Userinfo not going to be the token endpoint going forward especially if we dont want to mix personal info together with actual visa information, ga4gh claims.
- MB: this is just a restatement of what is in v1.0? It's not that token returned from userinfo, what is current specd in v1.0 is returned, a JSON object that has an array of visas in it.
- AP: we need to come up with a clear name of that as an entity. Do we want to deprecate that in any way? We are proposing token exchange mechanism that we get back signed JWTs.
- MB: my understanding that getting backed a signed thing containing visas from userinfo was only in the NIH 1.1 implementation not in passport v1.0
- AP: mentioned in the v1.0 spec but not fully spec'd out.
- AP: we could say only allowed you to get passport content as document.
- TC: in favour of that, if all v1.2 talks about is a new token endpoint some implementations can continue to use v1.0 and implementations for some time, the spec should focus on the right way to do it which will involve signatures for sure.
- Exchange flow: doesn't ever distribute initial scoped passport beyond client application. Initial PIDC token only meant for the client, only audience it could have is the client, not meant for sharing as peak of the power.
- In this flow passport token used as a bearer token though we haven't solved issue of some passports as bearer tokens could be large.
- TC: agreed that work order idea was saved for v2.0,
- AP: more just setting up generic end point, could take out word work order, part of power of this is to do different types of tokens in the future.

Summary of work-order

- We know that the main goal of what we've been doing in these meetings, confusion about the clearinghouse, how does that get the token? Is it always going to bethe client doing this flow, or is the clearinghouse removed from obtaining a token and receiving and looking at token. Concerns over confusion in spec. Also concerns of a really powerful token that has all of authority of user. Here tried to create second token exchange flow, by exchanging the thing that we call at least for now a passport scoped OAuth access token. That something else can fit a variety of different needs that someone has. Downscope the permissions of what data can be accessed by that token. You may want a token that can fit into amn http header so can use more traditional in oauth settings.
- May not have all solutions in next version byt token exchange endpoint lays groundwork and work order token will be tackled in v2.0. Specifically downscoping is a major concern for work order token, gives access to just what you need for a particular research activity.
- DV: one of the things you said, today you only get a passport scoped oauth access token, is that what we are calling the passport? Right now in my flow, i get an access token (oauth) to call user info endpoint to give me the actual passport. Still this passport scoped oauth access token, what i thought, that isn't the passport itself
- MB: yes accurate technically but confusion is which is the passport here? Payload back from user info? Community was confused as to which was the passport
- AP: especially when start to throw in a third concept, passport content now as a signed JWT, now 3 concepts all conceivably called a passport. We need to give names for all of these 3 things.
- TC: first one is standard OIDC access token, NOT a passport then use to get to token endpoint.
- AP: yes i called that passport scoped OIDC access token, current spec called it passport scoped access token, so i just added OAuth
- DV: those words are accurate in meaning a particular thing
- AP: following the exchange, user instructs the client, token exchange, URL encoded and only put in requested token type to be done. We need to better show that this is decoded base64, linkage between representations
- Use phase then: client just uses the token as a bearer token and decisions are made
- Does anyone disagree? This was my interpretation of my understanding
- TC: need to make sure it maps onto known implementations, does it represent everybody's needs? We need to validate that. How would we map client broker, visa issuer onto RAS and Terra for example? Same exercise for ELIXIR and some of the others.
- MK: steps are correct I just think that the yellow rectangle in the middle should be after the written assigned visas for user message. All other rectangles show something that happens before
- AP: yes I should come up as a colour scheme for representing posted and return values
- TC: perhaps as we agree on specific vocab of each thing and details of each different thing can be elsewhere in the spec, doesn't need the yellow and gray boxes.
- MK: i like it in place

- AP: theoretically make content of yellow boxes to make a flow of an actual story whereas the spec is super abstract, concrete example in this flow. Warnings at the top saying check the spec too!!
- TC: could leave out some details, ellipses maybe
- Put one or two attributes that characterise that bit of data
- MB: we might want to lean on example using DRS using the new passport or token endpoint that accepts a POST and you can include the token in the payload, we can document.
- DV: it is called a passport in the DRS spec
- MB: is that being used now by NIH in any of their DRS servers?
- DV: couple of months and something be in production
- KR: Doug working on it and NCBI and NIH will switch over to it,
- MB: no more comments personally it looks like what i was imagining, kudos to andrew for putting it together.
- AP: we need martin to have a look at the callback one and confirm that it matches ELIXIR's, the non-token exchange view of the world.

Vocab/terminology

- TC: as for next steps, Andrew had a few edits to make but do we need to argue about any terminology right now?
- Will help writing details of the spec
- Passport access token: precise name?
- MK: i dont like it contains access, it means somehow linked to oauth which it is not
- Passport token? Or Passport JWT token?
- TC: i used aai token as a placeholder
- Passport JSN and passport token other one/
- AP: agree, passport as abstract conceptual thing, nothing concrete. Passport tokens and passport JSON are two formats of that abstract thing. Or passport JWT and passport JSON
- MB: gave it a token type to be used in token exchange parameters, would the content be exactly what you would get if you requested user info in JWT format?
- MK: I think a bit more maybe
- MB: if different we need different names. More adjectives in name?
- DV: passport as the content, is there a case where two types would be different?
- JWT more content than JSON? Is there a case?
- AP: use for for JWT to have less content than the other one, point of downscoping etc to reduce the content
- KR: discussed last year, silent on some time to sidestep these naming discussions which token gets called what. What we did to re-iterate we took v1.0, user info actual user info stays in JSON in RAS, bundle of visas into one single JWT (only change we made) so you had something you could pass around as opposed to bundle of things to pass around. We have that fairly widely used now, several months now, in play. And whatever we do here i want to take pains that it doesnt introduce more confusion. What we have been talking about going toward work order, passport would stop being token that you

pass to DRS and instead be used as token awarded to the user upon login through the UI client, use that passport to build a workorder token that is scoped down and isn't fitting into the model any place on this graph. What we send to the DRS later on and with that, we don't care so much what things are called, other than we have lots of documentation and months of contracts that have been written around terminology. People do look to GA4GH to get some terminology

- Passports if they end up staying on this course fine. Passport we still think of as a single token not as a broad concept
- AP: so two concrete things a passport JWT and passport JSON, those things?
- KR: passport JSON not output of userinfo, user info is user info passport does not fit into that model. Recognised as faux paus of v1.0 to overload user info. User info doesn't belong anywhere in a passport. Passport should not contain personal information
- MB: we need to extend this, next step what is the format of token you get back? What is the token type called. Agree what is in it before we know what the name is
- DV: is passport of JSON concept useful?
- AP: currently used by ELIXIR so how do they want to go forward
- MK: you don't want to break backward compatibility with v1.0
- MB: do we need special name beyond user info?
- TC: v1.0 does allow to go to /userinfo as a path and use that standardised mechanism, somewhat wrong, shouldn't put human PPI inside of a passport but still go to userinfo endpoint to get the passport and visas. Conceptual mismatch but it sort of works. Doesnt mean you are leaking PPI, you had to go to same token that returns PPI
- KR: then you ignore it because of the access token, take the OIDC access token, authorises you to contact userinfo and get access to user info, what OIDC is all about. Same token we used to get at passport but they are separate things, someone dealing with passport doesn't necessarily have access to user info. Why we broke off to have separate passport and OIDC is the uber token that gets you everything about the user. If we can use the model that upon log in we get a token that is bearer token that is fragile, not usable for CL delegation. That instead we handle the CL case and post-authorisation case, really clears up the muddy waters from my perspective.
- AP: path forward but we still need to take into account what ELIXIR does and widely implement v1.0
- KR: not to pretend that v1.1 existed but it just never adopted.
- AP: v1.2 then you want to have backwards compatible existing production system. You have to do same respect to ELIXIR representation in v1.0
- KR: i do
- AP: attempt to diagram what ELIXIR does in v1.0
- We need to name the things that ELIXIR does as well
- TC: passport JSON, is passport JSON a JWT or something different?
- AP: unsigned passport content. Do we need to distinguish between content and back from user info is not passport as it also has PPI. do we have user info JSON and passport JSON? Martin?
- MK: user info returns JSON object, list of visas i thought to be the passport. Other claims, and one claim contains visas

- MB: user info payload as described by v1.0? Does it not have a home conceptually in what we want people to use in the future
- TC: Ga4gh_passport_v1.0 claim?
- AP: we might want new things in the future. Not changing visa format or claims format so stays as Ga4gh_passport_v1.0
- TC: new token, not even clear right now, is it itself a new JWT
- New token is a JWT and it has this claim in it?
- DV: how about what is in the JSON is a passport claim which is also a JWT which contains a passport claim, like issuer and so forth.
- DV: passport claim is good as it says passport
- KR: reminder of previous discussions, visa claim inside the visa, claim inside of a token, embedded token itself is a visa, not the visa claim, visa claim ga4gh language and controlled vocab part of the visa, for custom visas all of data is outside fo the claim, visa is the token, not just that claim.
- KR: visa well spec'd in comparison
- MB: rough consensus calling this array of visas or inside a JWT a passport claim?
- MK: still don't know to call token, signed passport?
- KR: NIH implemented signed passport, think what you are doing JSON array of visas, we can call that a v1.0 passport. We did v1.1 as we wanted that to be a token, we put inside another JWT and signed it and called that a passport
- MB: what we do in v1.2 do we want it to be signed passport token same as v1.1 or will it need to be different content, specifically for the passport token?

Let's pick up here next week…

2022-02-17:

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation): Kurt Rodarmer (NIH), Martin Kuba (ELIXIR-CZ), Tom Conner (Broad), Heidi Sofia (NIH), Max Barkley (DNAstack), David Bernick (Broad), Mikael Linden (ELIXIR-CSC)

Apologies: Andrew Patterson (UMCCR)

	Actions Arising	Assigned To	Deadline
1	We defined our to do list going forward:	All	Ongoing

	1. **Sequence diagrams for two scenarios (centralized and distributed)** 2. **Edits to AAI to describe new token end point** 3. **Edits to DURI spec to describe actual representation of the token - *compact representation* if goes into headers (passport content edits)**		
2	Alice action: registering the ga4gh URN namespace	Alice	Now taken up with GA4GH TASC
3.	Create two PRs on AAI, one sequence diagram with v1.2 in name? And then a token exchange PR that would have the framing. Plus one sentence on DURI side to change one sentence	Tom	Done: a map of how we can get the 1.2 spec done
4.	Alice to come up with a Passports workshop proposal for group review	Alice	

	Agenda Item	Person/Time
1.	April Connect session plans: https://docs.google.com/forms/d/e/1FAIpQLSesyyTmernUT3T2fBBwuJGlBEgH806rAE9lQzOnmewTZSFFRA/viewform	
2.	Hackathon efforts and new attendees to the meeting	
3.	Check in on the repos locations	
4.		

Minutes:

Connect

- Focus on v1.2 Passports

Hackathon and meetings

- Happy to open out meetings now
- HS: Now is the time to really integrate with DRS and later TRS, coming up with something they can build against, it's a good time to do that
- NIH is really committed to a zero trust model so all the effort to get to this point of agreement has been worthwhile, but now all the pieces have to come together so implementers move forwards

- KR: work order token advance towards zero trust and this is a direction that NIH wants to pursue, the other work streams need us to tell us to do something so they can get on with it. From our standpoint and NCBI and working with the tokens and with DRS, agree with heidi we need to be looking at it from a larger level.
- HS: needs to be an international standard that can be adopted by many different groups, hard things to balance. Credit of everybody for the hard work to reach a place where there is an agreement.

Location of visas spec

- Andrew had set up some branches in repo for AAI using jekyll to serve out the content, that references the DURI passport spec from v1.0. Those two specs interlink each other.
- The right thing to do is to make the minimal edits to describe the token exchange end point on the AAI side and then on the DURI side to put in PR and hopefully not any resistance for any content changes.
- DURI side describes content of the token and specifics of the claims and if move into different representation. We could lift the spec and put it into AAI side but will be a journey to get there.
- Two incremental changes to the two repos and hopefully get to agreement.
- Andrew did a PR a while ago that has a sequence diagram - good thing to incorporate in the spec, not dictating as an exact sequence but example of something the spec supports. May not represent all scenarios we have discussed. Shall we put more in there? Should we have one centralized model and another more distributed bearer tokens, lots of trust between different institutions. Helpful to agree on that first as this is what we are driving towards.
- What does everything thing? In agreeing on this in the next week or two and into spec
- +1 from MB feedback was not sure how passport can be used.

- **General to do list**
    1. **Sequence diagrams for two scenarios (centralized and distributed)**
    2. **Edits to AAI to describe new token end point**
    3. **Edits to DURI spec to describe actual representation of the token - *compact representation (clarify are we using this?)* if goes into headers (passport content edits)**

- MB: reference relevant RFC and referencing additional parts of passports to flesh out details of token exchange

PRs:
https://github.com/ga4gh/data-security/pull/43
Sequence diagram:
https://ga4gh.github.io/data-security/1.2-draft-sequence-diagram/aai-openid-connect-profile#appendix---sequence-diagrams
PR: https://github.com/ga4gh/data-security/pull/52

- MK: would change Seq diagram a bit, put there different end points like authorisation end point, token, user info endpoints.
- MB: separate visa issuer, is that helpful?
- MK: we do have several visa issuers in ELIXIR so emphasis possible to have multiple of them.
- MB: some text then that makes it clear or maybe we can colour code so parts that are explicitly spec'd are one colour and others implementation details that are likely to exist but not necessary are one colour.
- NIH has special dbGAP visa
- MK: visa issuers it says but just one data owner but it can be multiple data owners.
- TC: I can make these edits or Andrew can, does this expected flow represent the expected flow for everyone who can use it? Is it useful to have a second one? It drives the point that you are not required to follow the spec
- MK: yes have two, one that uses token exchange and other not using it
- MB: end usage as well of getting data, right now just say clearinghouse not specific in a real world usage sense e.g. DRS server (clearinghouse), do we have another example other than clearinghouse.
- TC: could also represent htsget, if a real case we should address that one too
- MB: we should also discuss what the tokens look like more
- MK: we decided not to use the compact format, keep grant type.
- MB: can we put example references of different types of tokens we use.
- TC: yes allow to see how sequence on one screen
- MK; we need our content type for the passport, different registry but probably a very similar process, like RFC for specifying JSON based access tokens, specifies its own content type just to show that it is some concrete type of JWT. we should define also our own
- TC: IAN registration?
- MB: would that come into play if you had an endpoint that would return a token from wrapped in JSON.
- KR: subtypes of JWTS not understood generically by off the shelf parsers, even if spec conformant
- MB: worth testing how commonly used libraries, if they fail if they see a header they don't recognise or they ignore it, to see what happens
- TC: shall we take Andrew's branch, agree on it and merge into v1.2 main and iterate on it. Do we like multiple branches?
- MB: sounds reasonable to me
- Checking overall architecture: https://github.com/ga4gh/data-security/compare/master...1.2-draft-main

- MB sounds like we should iterate on Andrew's PR and merge with an appendix of how we think this is supposed to be used. Other changes best suited for new PRs.
- Can we crowdsource the general structure of how we want to frame the introduction of the changes.

- Introduce token exchange end point first as new intro to spec, separate PR with new token formats
- TC: wondered if the best way is to put token formats into PR DURI
- MK: shared this: https://github.com/ga4gh-duri/ga4gh-duri.github.io/blob/master/researcher_ids/ga4gh_passport_v1.md
- Defines the visas not the passport
- TC: very specific about visas not the passports.
- MK: i would leave this one as is maybe change the start as definitions visas rather than passports in AAI spec add intro to token exchange endpoint, alternative way to get passport visas.
- MB: messy if one of token formats is JWT that contains embedded visas that contains the big token, whatever spec defines that token needs to reference visas and that becomes aai then you have passport and aai specs having circular references to each other.
- MK and TC: it already happened though
- KR: AAI about passport token technology and DURI about semantics of some of the claims
- TC: maybe let's keep the distinction going forward forever?
- TC: David B did want them to merge after v1.2, as part of v2.0. That turns into small PR on DURI spec, acknowledges there is a v1.2 in the beginning and that's about all.

2022-02-11

Chair: Tom
Attendees - Name (Affiliation): Kurt Rodarmer (NIH), Martin Kuba (ELIXIR-CZ), Tom Conner (Broad), Heidi Sofia (NIH), Andrew Patterson (UMCCR)

Apologies: Alice Mann (GA4GH), Max Barkley (DNAstack)

Note, the proposal/specification documents for work-order token are here:
https://docs.google.com/document/d/1t9I99qc3elojSWA340rvGIR6O-9pvr3Zw4ZzpqTlbHs/edit#heading=h.mb53z5y4943m

	Actions Arising	Assigned To	Deadline
1			
2			

	Agenda Item	Person/Time
1.	Passports workshop and spec work on repos, decision log	
2.		
3.		
4.		

Minutes:

- Discussed branching/github mechanisms
- Discussed the location of the DURI visas spec and where it should live - and does it need to be edited for 1.2? Martin thinks it will probably need some language clarification.
- Martin went through initial experiences with doing token exchange
    - Elixir stack had no obvious spot for implementation so he is experimenting with other stack
    - 4 issues he floated
        - URI needed for token type (discuss with GA4GH about how they want to do)
        - Should exchange reject non-ga4gh scoped token in exchange (answer yes)
        - JWT returned MIME type (should it be passport+jwt - probably?)
        - Aud and resource params mentioned in passport spec (Martin thinking probably should not be mentioned as they are in the master token exchange spec)
- Andrew mentioned that the official oauth JWT access token spec went to full RFC late last year - possibly should at least give it a read in 1.2 timeframes to make sure it doesn't contradict anything in passports https://datatracker.ietf.org/doc/html/rfc9068
- Group discussed sovereign self identity that had been discussed on DURI call and agreed it was probably a fair way in the future (keep an eye on but no immediate changes for spec thinking in 1.2 timeframes)
- Revisited DRS

2022-02-03:

Note, the proposal/specification documents for work-order token are here:
https://docs.google.com/document/d/1t9I99qc3elojSWA340rvGIR6O-9pvr3Zw4ZzpqTlbHs/edit#heading=h.mb53z5y4943m

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation): Kurt Rodarmer (NIH), Martin Kuba (ELIXIR-CZ), David Bernick (Broad) (joining later), Max Barkley (DNAstack), Tom Conner (Broad), Heidi Sofia (NIH)

Apologies: Andrew Patterson (UMCCR)

	Actions Arising	Assigned To	Deadline
1	Tom to speak to Andrew re Jekyll and start new PR for v1.2		
2	Martin to give a go at implementation of token exchange		
3			
4			
5.			
6.			

	Agenda Item	Person/Time
1.	Passports workshop and spec work on repos, decision log	
2.		
3.		
4.		

Minutes

Communicating progress

- v1.2 introduce token exchange will be a small change
- MK: i will try to reach the spec for this and implement it
- TC: if just token exchange and not the work order

- Edit to existing repo to v1.0 ?
- MK: but without adding the steer to v2.0 about work-order then people will try to use it for authorisation.
- We will maybe work on detail in google docs and then move to github so people can publicly comment on v1.2

FASP query

- TC: yes we can detail that the intro, the vision for v2.0 and how to use the tokens
- Our impression from this from FASP hackathon, they need the work-order token: https://github.com/ga4gh/data-repository-service-schemas/pull/381
- MB: potentially if we do v1.2 and talks about token exchange, document at least one token type, we talked about two last time, but we document at least one token type where you get the JWT with visas embedded. DRS has been updated where it has some endpoints where it can accept passport token in the body of the request in anticipation of there being a giant embedded token. That is a viable option if a v2.0 is a year away. Still need some access token in the header but can send a passport at least in body that has info about the researcher. Short term recommendation
- KR:it has just dawned on people that if they have more than one passport then they just confused as to which passport they should send to a DRS server. Conceptually most of people involved in this phase of the project have not thought beyond that and considered that there will be a single passport. We don;'t want our RAS passports to be repackaged, or the visas to be repackaged. UoChicago says then we need our own passport and have a NIH passport so which one do we use. DRS in v1.2 introduced protocol to send multiple passports to DRS. let DRS find appropriate visas in bundle of passports but how does a client decide which ones it should send instead of sending all of them. Unravels quickly as the approach we took, the basic token system we have been modeling on doesn't handle this problem very elegantly. Same content that can live at 3 different sites will have different object ID, chaotic.
- MB: how do you figure out which passport you need from an object but abandoned that in favour of how do you exchange tokens and what type of new tokens you need. At some point someone will need to go back to that. But which passport needed for an object, v1.2, token exchange and new embedded token you can send to DRS, will it partially solve the need and work on work-order tokens.
- KR: i think martin is right, they are asking for a solution that comes through the work-order effort. There is a facility in DRS to send the tokens they have and not need to know which tokens to use. All tokens I envisage right now will be a single passport.
- DB: i don't talk to DRS people as much so don't know much about this PRs.
- KR: there was an assertion made that our group had discussed it and decided, but KR said was the first I had seen of it. Has anyone else been discussing it?
- TC: i know that piece of presenting passports to DRS is in flight right now, not settled it yet. What does it mean from the spec?
- DB: this PR has not been discussed by anyone i know. The document is about a year old.

- KR: throwing out there the idea that you can add in options access method, everyone seems to look for the easiest way to solve their particular problem. We aren't in a position to deliver what they are asking for, useful to understand the problem as we work on developments in the passports.
- MB: useful links. This doc has the stuff we talked about a year ago:https://docs.google.com/document/d/1ISRIJRFSIB8EMww_yOY6hWkT6O7jDABdmxegsmFBD24/edit#
- We stopped looking t that API when we focused on what tokens we need and fit into headers not immediate concern from this call.
- MK: why is it a problem? First you get a passport, which data objects the user has access. You know which passport you need for that object, why need opposite method? You need to access object so looking for the passport you need?
- KR: process of discovery doesn't necessarily involve a passport. Possible to discover DRS IDs without having access to the IDs to the objects you identified.
- MK: object does it always belong to one owner, or multiple copies and you may need different passports and accessing different copies of it.
- KR: good and reasonable question, that is a legal issue from our standpoint at NIH. there's the content creator which would be the subject, there's the publisher that is NIH, own publishing rights over content and reseller which are the various places that host the data, each has own concerns but for NIH and RAS our token represents user right to access the content of that instance. That can only be authorised by NIH in our case.
- MK: where is then the link between the data and the publisher?
- KR: in our tokens the ID of NIH is there in the form of the signature, identification of the dataset is in there as well. No identification of the hosting system. Technically if you were to be pedantic about tracing all of the authorities and responsibilities and concerns, the hosting system has unique authority over whether you will allow access to the hosting system but not auth accessing to content. David'd system can host NIH object and he can allow access to system but NIH also needs to grant access to the content. We may need to look at modelling both of those ideas. Not clear from a DRS ID that they are talking about content. All about specifying an instance on a hosting system. The DRS ID if it were modelling an content identifier then it would be location agnostic, where are the instances I can access of this object. Under DRS we can have 3 or 4 different DRS servers each giving out own ID describing the same content, get's confusing if talking about

- MB: Regarding the earlier question about 1.2 of "Should we work in a Google doc or GH?", here is a PR that tried adding token exchange and "Token Containers" that David created and I helped edit from a year ago that might be worth resurrecting: https://github.com/ga4gh/data-security/pull/43

- DB: happy to kill this and start a new one if you want. We can reference this previous PR in a new one.
- TC: andrew had stood up a jekyll we could use that. It's in the GA4GH pages. We could use that as a physical place where edits go and refer to David's, and nail down some

token exchanges. Lay our work-orders even if not in v1.2. Once in PRs we can now argue over the specific edits and we can use the reviewer stuff inside of github and do hard work of getting to approving the changes

- Decision to go forward in this way
- TC: MK you will implement it? That sounds great
- MK: looks like something should be easy so I will try it, I can do it on ELIXIR AAI so no token exchange so far so won't break anything by adding it.
- ML: what kind of authorisation from the end user should be requested for TE? Do end user need to authorise TE or just something that happens in backend, visible to user?
- MK: invisible, spec says access token exchanged for security token, no limit that it must have a specific scope or anything.
- ML: does the user need to know? Should they be aware of, now some client is request a token exchange that led to new token replacing work orders.
- KR: extends consent. Clients should be working with work order not passports. Passports for user to use, could involve consent. Not there but once the work order is created, exactly user consent for the token to be used. User authorises a client and only that client creates a work order token
- MB: couple of options at least based on v1.0 does, part of your consenting to do your flow with client. Another option add another scope to v1.2, GA4GH v1.0 gives you access to all 1.0 stuff, heres another scope with extra consent messages when log in to let them know they can also do TE. don't think covered in TE spec so we would need to add it.
- MK; who or which entity will ask for TE, some client and will ask for some TE for WO token. Delegated to WES, this service will find out which systems to use, and what should go into the work order token, client and user interface may not know specifics about TES which will be used.
- …..
- MK: do we leave the specifics to be figured out but WES?
- KR: researcher and researcher's agent (client) has the responsibility to gather up info to say at very least this is what i want to work on, these are objects of my work order. That has to be known by user and user agent before WES gets involved
- ML: im trying to figure out what does the very first client of passport broker need to know and grants the OIDC authorisation work flow, all info needed to be placed to tokens so that user is informed and consents needs to be place in that phase.
- KR: use case in dbGAP, user go to run browser and run selector and file selector, browser our catalog and find objects they want to work on, go through and select a bunch of checkboxes and can download as a file with json description of the selection. Captures it's amazons idea of a cart, in some cases you may need a passport to browse the info but between your objects you want to browse, enough info to create a work order from two things, and pass into work flow WES as well as description to what you want to do with those things
- TC: when browsing done and user done, start researcher and work order token will need to be made. User interface must have knowledge of what downstream DRS or WES

server, what they need in order to turn the data over. What kind of token/selection step needed

- KR: user agent doesn't necessarily go out and scrounge up authorisations you have, you come with your auths and work in those constraints as can't escalate your permissions. Merge together and create work order, may not describe actual work outside of scope but has enough info to go onto another stage and create token that carries authorisations that you need to hand over to workflow. WF given its limited set of auths that now belong to workflow not user, scoped for how many days workflow has to complete its task. A work-order in other industries has slightly different meanings, usually tasks workers as a result of a purchase order.
- TC: that concept is fundamental, the auth of user to take passport to the WES server user auth and auth of wes to carry out the tasks and process data is a machine auth or that wes server. And the token itself doesn't want to be a bearer token, separate google auth token required, not just a bearer token that anyone can take in and use.
- KR: it's an assigned token.
- MB: v1.0 user consents for Clearinghouse to see user and signed assertions about them v1.2 additionally user to five permission to get a signed copy of that that it is allowed to share with other systems to run on your behalf.
- KR: yes I agree. Martin called it a delegation. Sharing mechanism in real life like a power of attorney, when you are contracting with someone else and act on your behalf, you grant them your authority.
- If passport used to create derived token, passport can carry that authorisation.
- MB: difference is if you say user has permission to get work order tokens or the client has permission to get work order tokens for this user. If DNAstack workflow system doesn't have new scope, it cant get work order tokens for any users. What entity do you want to restrict?
- KR: i'm fine with it being a scope, as can already gather user consent when logging in.
- MK: there may be a different consent for getting Work-order tokens in general or getting a specific work-order token? Ask the user if he agrees this agent can access the data on his behalf. Does the user want to control where data will be processed? Or trust the system to process it in the right place or if both is possible
- MB: what this is giving us you can get this thing that is proxy for work-order token, you can sned this to a DRS along with access token that gives you access to DRS server with permissions to what data you can access. User consent just being able to get any WO token, in order to use at any place, have to do a flow to get access token for that system. That is control to them to using a particular DRS server.
- TC: seems more workable than asking for them to authorise with data or work server. A little crazy from a user perspective.
-

2022-01-27:

Note, the proposal/specification documents for work-order token are here:

https://docs.google.com/document/d/1t9I99qc3elojSWA340rvGIR6O-9pvr3Zw4ZzpqTlbHs/edit#heading=h.mb53z5y4943m

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation): Kurt Rodarmer (NIH), Martin Kuba (ELIXIR-CZ), David Bernick (Broad), Max Barkley (DNAstack), Andrew Patterson (UMCCR), Tom Conner (Broad), Heidi Sofia (NIH),

	Actions Arising	Assigned To	Deadline
1			
2			
3			
4			
5.			
6.			

	Agenda Item	Person/Time
1.	Let's take up from the email discussion and feed into the specification	
2.		
3.		
4.		

Minutes

Note, the proposal/specification documents for work-order token are here:
https://docs.google.com/document/d/1t9I99qc3elojSWA340rvGIR6O-9pvr3Zw4ZzpqTlbHs/edit#heading=h.mb53z5y4943m

- DB: Have agreed to get something into authorisation headers, but need some clarity on what we are delivering?
- Original token, called passport access token, use it to talk to userinfo and other endpoint
- New endpoint result: needs an explicit name, used as a bearer token. Decide on name and what it looks like
- Are those the two immediate goals? Do we have agreement?

- AP: yes but new thing you are looking at, bearer token and thing called access token and passport access token that is a passport, not sure we will survive that. Needs wording correctly
- DB: original access token, OAuth handshake access token, new token is used for access BUT NOT OAuth.
- AP: maybe Bring OIDC into original name, OIDC passport token to clarify first one you get
- DB: we still keep userinfo thing and if you want to use it it is still there, it doesn't break backwards compatibility, but if want to get a token used downstream in headers, that is available.
- People can advertise we only support v1.0 or call out if support v1.2.
- AP: only other issue i have there, guy who wrote that spec into conformants suite of Oauth. As of recently, userinfo endpoint not allowed to be used except by client who gets that access token. Downstream resource servers, inherent call back mechanism we proposed as part of v1.0, access goes out downstream, someone can call back to broker on userinfo, he says is fundamentally not allowed in reference implementation. Read OAuth spec only thing allowed to use that is the client.
- KR: we've been saying that for a while.
- AP: can say we can modify oauth spec then?
- MK: access token is a bearer token so anyone can use it so not limited to the client
- AP: access is a bearer token but userinfo spec says only client is allowed to use it.
- MK: problem with OIDC spec, doesn't say how RS gets infor from user, expects these are same organisation. But in ELIXIR and other projects, usually have auth server provided by somebody and RS by somebody else. Modify introspection endpoint to return.
- MK: access token as input and returns if access token valid or not
- MK: introspection endpoint is defined in OAuth specification
- Introspection endpoint called to get info back on it. If it's valid
- AP: who is then using the userinfo from RS?
- MK: the client has to use it as specification says that there is an ID token released but it may not contain user claims, so useless. Used in some scenarios for validating some signatures.
- AP in currently deployed v1.0 passports that exist, what currently exists? NIH not doing that way, no downstream RS using the userinfo call in NIH?
- KR: they can't
- AP: is ELIXIR currently doing t he callback to userinfo endpoint?
- MK: i don't know what the client does

- AP: but RS distinct from RS?
- AP: do we want to confirm that that is what they want to do? Clarify spec as to what it says
- MK: i will check OIDC spec
- KR: NIGH was one of the voices in signing v1.0. As essentially a compromise and start working on v1.1, that is when progress seemed to stop a after v1.0 but we don't accept v1.0 as viable. Idea of rolling back to v1.0, we should be careful about. It needs repairs. To me going back to v1.0
- AP: can we get an understanding of what is currently used in v1.0, that is our starting point of what has to go forward.
- TC: a lot of time spent doing this. Let's focus on a v1.2 document
- AP: how can we maintain backwards compatibility without knowing what v1.0 currently does?
- MK: calling userinfo and getting just JSON. assigned JWT and we have to configure it in our implementation. We never configured it for anybody
- AP: signed JWTs you never get from userinfo and in v1.2 introduce token endpoint so you can get signed JWT and access bearer.
- MK: where is someone getting signed info from userinfo as the token?
- AP: it's in the spec…?
- DB:NIH project has a semi trust relationship using RAS endpoint. Authentication user to system B, both use RAS and passport and they should be able to get a passport on one system within these semi trust relationships. That is the origin of this and it is a very good ask. How to make a transparent trustable authentication, loosely coupled environment form a circle of trust and trust each others authentications. Token passed around is to link that vision up. Make their own risk assessment on the ability to trust passports and/or visas they get from loosely coupled environments.
- KR: The work-order is still a bit in the future because of the requirement to provide evidence of client identity. 1.2 might be a nearer-term bearer token.
- MB: system you described David are using v1.1. Fair to say that no one in world is passing around OIDC access token between multiple parties.
- DB: yes but desire is there, some sort of JWT that says I have permission to view this thing, i've already authenticated with a system we trust, to give almost single sign on.
- MB: agree with AP that we deprecate that… and if you want to do it then go to v1.2.
- TC: new discussion on new tokenendpoint and work order token, it is workable for diverse different needs. Let's minimise how much reference to v1.0 we put into this new document. Lots of definitions, some were place holder definitions in v1.0. Passport is not really a thing in v1.0, passport visas is where the essence really is. Getting a really small spec is forceful but limited in scope, definitions and diagram to show handshake. Let's start over
- AP: but i think you can only get to that with an understanding of current implementations, we need sign off to get there. Australia has no existing passport implementation, two that we have implementations that we know of.

- MK: we approach it from other point than NIH. ELIXIR concerned with establish who is the user, we care about other types of users. Need to decide if the user is a researcher and there it ends. But this is where NIH starts. This is the point where we meet.
- AP: but this understanding is important when defining the spec. ELIXIR for example not inherently super large. Easier to understand to chart the way to v1.2
- MK: ELIXIR happy with v1.0 specification. We can simplify it a bit, don't like v1.0 it says two types of visas, access token visa and document token visa (check name), complicated.
- AP: is this not an opportunity to say no one uses embedded token visas then take that out of the spec.
- DB: the passing around access tokens to other systems. Thing that makes it challenging is that these are separate systems that are loosely coupled. Everyone using same authentication system, RAS.
- AP: happy if we delete things not used and gave clarity. Currently v1.0 is unreadable and unimplementable. That is my only requirement.
- TC: why I suggest we start afresh.
- Kurt wrote up a good write up of workorder and the properties in it. If we put that essence in how it is used, how the flow works into a new document, will be much shorter.
- AP: Work order spec completed is surely a year away. It is in early days of what is needed in the format.
- KR: i like pure OIDC to get your authentication and access token to get userinfo and token access, but not called passport, still think scope of GA4GH one of many scopes, i think passport wants to be a less powerful token than the original access token. So passport only gets you to data not back to userinfo. We have a goal of having our tokens not carry PII. don’t want a token that allows someone to go back and get your email and full name, does not qualify for our purposes.
- MK: i don't see a problem with having access token for multiple scopes, up to client to specify which scopes client asks.
- KR: but then the client shares that. It is the sharing I am concerned about. Whatever tokens gets shared should not be token authorised specifically for the client. If i go into webpage and hear webpage wants to get access to your profile…..
- MK: but exchange it can limit the scopes used
- KR: yes that is true, i don’t think that that is fundamentally different from what I was saying either. So we just want the token that is the passport, what RAS would want, no pathway back to PII.
- AP: some sort of agreement possible? But it is not written down, what is ELIXIR’s flow and NIH’s flow in a compatible forward looking world. What is the common shared flow to compatible to both implementations? We need a spec that you both agree in that is compatible in some sense.
- MK: v1.0 says access token is passport scoped.
- TC: only portion of spec though.
- AP: what is a practical flow. We have never come to agreement what are the first 3 REST calls that you both want to make? In australia we need to call either yours or theirs and at the moment we don’t know what they are.

- MK: what is the problem? Spec is OIDC used and passport is something written from userinfo as a user claim.
- AP: NIH won't allow OIDC access token comes from that flow, first flow get PIDC access token. Europe, that token can be passed and call back to userinfo by RS, client all sorts.
- NIH: not allowed to pass that anywhere and can only be allowed to do calls as a client
- These are fundamentally incompatible.
- KR: Martin how does that affect GDPR? What is the GDPR implication of passing around token that reveals user information.
- MK: user who decides that his or her personal information will be released to the client. User believes that client is behaving with according to some rules. (i think)
- DB: GDPR in general okay to do stuff with PII in GDPR you have to do it the same way. You have to inform people and they can delete them in 72 hours. You have to minimise it and up to data processor to decide what minimisation means.
- KR: entire security industry has incomplete model here. Not trying to fix that but point out that right here, OAuth concept involve the user and get into user consent to work with a client. Based on logging to facebook and not massive genomic processing. May consent to give email and name to log in page. But not same as saying i also want every service that gets involve to have access. That is not in the model. If we introduce a second step so we give initial user what they need and a step to give me a token that is appropriate for other sharing purposes it can be done by any means we want. That seems straight forward.
- AP: yes I agree. It says client is only one that can use access token for userinfo.
- DB: why we backed off on passing the access token around. What is something that is derived can you pass that around. My interpretation is you can do that in a loosely coupled system with a lot of trust.
- KR: requirement is that passport derived token can be signed with same source of authority, carries same weight, if signed by someone else not good.
- AP:can we say ELIXIR happy with access token, then can we come up with first 3 steps that is compatible with someone using some sort of token exchange and those not using OIDC access token. Can we get some common language around that. Is that a spec that is compatible and implementable?
- TC: tried to write a few bullet points to capture that. I am sure they are only 80% right.
- AP: KR, when do you think a work-order spec would land?
- KR: I want to prototype it first. Ability to create one is straightforward with two big humps. In next few months maybe.
- DB: Note: we can ditch the idea that some sort of token can be passed around and only have it as an errata/faq item (like it is now) and pre-supposes that systems that agree to that are semi-closed networks.
- KR
- MB: v1.0 + some token that is sort of like userinfo returns but you get it from token exchange endpoint instead
- MK: how would it be used, for what?
- **MB: in v1.1 returning all of visas in JWT like embedded passports visas, return from userinfo instead of just JSON. We have v1.0 where do OIDC and get OIDC**

access token, you can also exchange OIDC access token with token exchange endpoint… incremental progress.

- KR: but from me (not discussed in NIH internally) idea of work-order token is what offloads need to carry visas instead passport token. V1.0 overloaded everything and as long as we can work toward work-order token and can specify what you are and carry all the visas that you need. Then we can discuss a lightweight passport token. Very close to v1.0 model but wouldn't be using an access token that gets you back to the userinfo.
- DB: what max said is exactly what I propose for v1.2: that /userinfo doesn't change at all or how we interact with it.
- AP: is that acceptable to both environments? Same flow, same visa, same passports, userinfo used same way. Document in the spec this is a callback.
- **MB:** but what is kurt suggesting may be small delta but gets us something bigger. V1.2 adds token exchange,and then what type of token are you exchanging for.
- KR: It looks plausible. Such a token would not necessarily support downscoping, but the work-order token relieves that burden from the passport.
- AP: introducing tokenex change endpoint you can have lots of different types of tokens
- Token exchange to get me a downscoped thing.
- MB: imagining martin's criticism is request new access token, OIDC without openID scope.

KR There are several considerations that we juggle at NIH:

- 1) downscoping - this is one reason for carrying visas within the passport. Custom-downscoped tokens require server-side state which is a security risk.
- 2) refresh mechanism is clumsy in OAuth - only the client is supposed to have a refresh token, but when the tokens are delegated/shared for performing work, the timeout will affect the delegated worker who won't have the refresh mechanism. We want to address this

MK

- V1.2 would introduce token exchange that would release same visas as userinfo that are signed
- V2.0 adding the work order token?
- I am fine with it.

DB

- Sounds like we are all good, but sure option to only return

2022-01-13:

Chair: Alice Mann (GA4GH)
Attendees - Name (Affiliation): Kurt Rodarmer (NIH), Martin Kuba (ELIXIR-CZ), David Bernick (Broad), Max Barkley (DNAstack), Andrew Patterson (UMCCR), Tom Conner (Broad), Heidi Sofia (NIH), Mikael Linden

	Actions Arising	Assigned To	Deadline
1			
2			
3			
4			
5.			
6.			

	Agenda Item	Person/Time
1.	Jeremy: FASP Hackathon	
2.	Refresh for the latest stage of work from 2021: https://docs.google.com/document/d/1dQ5tL4fdpRqhxHvX4HNjmYgvrGStgm1SWSMsSkawGes/edit	
3.		
4.		

Minutes

- Jeremy: FASP hackathon and test bed
- KR: test application, actual binaries or do you mean application in a different sense?

- JA: the former I think some application like a command line app that you would say run my test bed and then give it end points to say a DRS server and/or a passport server. Conduct a number of use cases/test scenarios
- KR: with automation, in obtaining a legitimate passport for the operation from automation problem, CICD automation not supposed to get a passport, needs human intervention, if you get a passport by human intervention it has a limited lifetime so you end up seeing your passport expired in the pipeline. Just wanted to point out in the complications. We will participate in hackathon and offer a few of the tests that we need and a few corner cases, in addition to the obvious
- KR: issue with taking anything that isn't an official token, otherwise easily forged in CICD pipeline. Depends on how strict you want to be on that, forging your own passports in order to make the system automated, is something that doesn't test how your system behaves with real passports.
- AP: test bed suite more like dev interop end rather than running against my test suite, with whatever quirks of my system.
- KA: anyone else want to weigh in, is this of use to overall design of what we are scoping out? Useful to other implementers of passports? Model/reference that they can go back to to see if technically matches the test bed
- TC: good idea, dangers that Kurt mentions is worth considering but useful project to identify bugs outside core token spec.
- AP: great if there were kind of like permanently standing up reference implementation end points, go to CL test bed, written my own DRS server and run test against DRS but don't need to implement Passport server as well, or do Passports server and permanently set up DRS server. Could be a standard endpoint that you could specify. More and more permanent reference end points at GA4GH would be good. Cost considerations however.
- KR: i think that is right and goes as far as to say we need to publish sample tokens that can be used as reference tokens. Publish keys and make sure never accepted in real life mechanism but output and behaviour expected. Building a system that you can verify is working according to spec is slightly different to what you can put into production. Emphasis by making the clearinghouse separate from sort of a module that you can interchange, you can use a clearinghouse that is able to accept these illegitimate reference tokens that wouldn't be accepted in production.
- JA: yes looking at that with GA4GH starter kit, already have DRS and VRS.
- JA: send a doodle poll to this group and then if interested in participating in the hackathon we can set up some times to meet. Appreciate any additional feedback as we scope up the test bed.
- MB: hackathon goal is to spec out what the test should do?
- JA: yes not develop the implementation level, can we get some documentation where we lay out what would this system look like.

- MK: How will we call the token?

- DB: Initial feedback that we are gong to have a token endpoint that can create a token passed around in headers
- Format of the token left up to us as a group will decide.
- Still have a small token generator, endpoint but people can ask for a larger one if that's what we want.

- KR: I think this is what we agreed on.

- MK: We need to say what will be the next steps
- 1. Decide the name
- 2. Then the token should not be a bearer token, should be an assigned token. How will we do this?

- DB:I thought idea is that people can have a bearer token so they can use it in pre-existing APIs

- KR: a while to go before any other use will be deployable, we do have to work in current paradigm. Will need to use the passport for all operations.
- MB: coming to an agreement on token end point and new kind of token and desire to be compact and then there was concerns that original compact token representation. Can this describe richness of current v1.0 token. MK had alternative compact representation. What did we land on what this token should look like? What does a compact representation will look like? Some amount of downscoping.
- MK: workorder token can have totally different format from the passport. What should go inside? Specify the datasets which will be used and probably the computing elements that will process the data, something like that?
- KR: what that does is it relieves some of the burden as to what we have been doing with a passport token, then passport token becomes gateway to getting to workorder. Bearer token for passport token as keep in TLS tunnels, a short term token used to get to the one that lasts longer and you do your work with. Tends to align more with my understanding of ELIXIR model, aligns well with the use of these tokens that's closely associated with the authentication. If working in pre-authorisation phase on bona fides and attributes then wouldn't necessarily get to workorder token for what you are doing. MK of EGA model that is all they are looking for.
- MK: EGA does not need the token just using userID. Up to NIH to specify what they need in workorder token.
- KR: we may have a large percentage of use cases for post authentication thing, so it's something that we can work on and elaborate and try to fold in. that's where we can concentrate the downscoping and actual use, all of concerns about whether the client can perform the downscoping. Passport able to be lightweight and does not need to carry explicit permissions within the token itself. Can be passed around in auth header as lighter.
- MB: there's a still a general agreement, workorder token, smaller, downscoped and fit in headers. Focus more on just being an access token for some operation of data.

- MK: last thing, NIH needs to put a lot of data into the token.
- KR: not quite, information is one thing, I don't think that the tokens necessarily need to be jam packed with everything, tailored and specified for the work at hand. Martin and I are the main proponents of this, but don't need to have full URLs to represent a boolean value, can be compact and doesn't have to adhere in any way to token format we've been using because it's going to be for a dedicated and custom use.
- Custom changes: except for preservation of OA, a lot of desires for custom formatted get shifted onto derived token and lightens burden on the passport token
- DB: passport token generated from hypothetical endpoints and headers
- KR: don't know if workorder token will be used in auth headers. Potentially use multiple tokens in a message, paradigm shift. Add header in as header outside of the protocol. I am working on AWS and google to get acclimated with ideas about taking a token that allows them to charge an account and have different or more flexible ways of billing. If we dont break out of single token does all in auth header we will never get anywhere. Workorder token go into a multiple token world.
- MB: is there not a desire at least in the medium term, still be possible to use it as a bearer token. Some applications require bearer tokens.
- KR: i was talking about the work order phase, that as a group we found more agreeable. If all desires to move towards workorder token then passport gets passed around in auth header that works with FIRE, challenge is need downscoping to use with this. Work out what security means with fire, not just accessing data at the source but is there any control once it leaves. Building aggregators that have no security whatsoever. Main point is we need to have a small token in auth header for that kind of backward compatibility

- DB: get to that to main task, which is how do we put things on paper to get new version. All agree to generate a useable token beyond userinfo endpoint which will remain. Shall we do a diagram? Should we draft language? What is the next step to move forward
- MB: we need the token format, if that token to solve that is workorder token then we need an example.
- AP: for workorder, how much of any current standards applicable? JWT for signing and custom set of claims? Or custom set of format? Any other standards that do workorder tokens? Macaroons, side tokens?
- KR: aside from my own work I don't know any, not to say there isn't something out there. What i proposed to NIH and got positive reception, is that NIH which is good at funding and using financial resources for things. We ended up proposing it for a standard, we would also supply open source software. Complication here, bearer token management not simple if try to use as general purpose tokens. Bearer have very few legitimate uses. NFT is latest craze here, an attempt to create legitimate bearer token. Except for very few cases intended to be unique instances, shouldn't be able to duplicate them with same effect. Often bearer tokens are misused from a security perspective, everyone does it as it's simple to manage. Just have to be careful to tip toe around security holes and try to avoid revealing the tokens. That's what we do at the passport level and trying to keep them in TLS tunnels. Matter of trying to keep the token hidden as long as we can. As start to do big iron genomic work we can't keep those tokens hidden. If all do is

log in and doing a search that's ok, once in territory of sending to CL tools you are in different territory
- We have that as a primary use case
- Broad uses a system where we have tokens that can't be forged.
- Threat model developer workstation fairly secure, if someone got passed our local endpoint protection then would be able to see those tokens and use refresh token and do many things. The protocol though and CL to use oauth is quite sound.
- MB: that threat model applies to a lot of things even if use message signing.
- DB: yes how i write it off. Make developer machines as secure as we can make them etc etc
- Weak link in CL tools using oauth is that it sits on the developer work station. Just like someone keeping a password manager on their local machines.
- Refresh bootstrap token every month and user has 2FA
- KR: if use passports in CL tools a passport that not only gets you to where you want to go and a different system, does that change the security model?
- DB: treat initial handshake as regular oauth and take token back to broker and get a refresh token. Client can continually get a token to get workorder token. Needs to go and do it again or if get a 401. Still in good shape for using in CL tools.
- BD: CL tool gets access token and presents it via perl or python request.
- TC: each consumer gets their own unique token that is not shared with other users.
- DB: refresh token needs to be stored securely.
- KR: each tool needs own refresh and access token. None of tools are user facing.
- DB: we do see user facing tools with that workflow all the time?
- KR: how does user get token that passes to CL tool?
- DB: CLI log in that does an oauth at command line. Sets up initial refresh token and then normal oauth consent screen, downloads to local file and system, refreshes access token on a 30 min basis. That is just sitting on hard drive in doc file, weakness.
- MK: every time exchange for new refresh token?
- DB: not sure, just saying what google command line tool does and we parrot that.
- MK: what to do if refresh token stolen? Get new refresh token and only used once.
- TC: stronger even than 15/30 minute window, not as good as one time only but still good.
- MB: last time i used google API they were rotating refresh tokens
- DB: oauth on command line can be done.
- MK:
- KR: exactly the point
- DB: do it similar to how google cloud does it, do regular oauth handshake get tokens then talk to brokers to get workorder tokens and use them downstream.
- TC: sequence diagram? Also what is in the workorder token
- AP: step after probably, proposal to have a new type of token. Kurt may want to drive that, what are the features, can we get those written down. Presumably it has stuff to prevent it being replayed. Can you write that down as a starter point?
-