GA4GH passport support in LifeScience AAI

In October 2019, Global Alliance for Genomics and Health approved the Passport specification, describing the syntax and semantics for expressing users' access rights to registered and controlled access data. This document describes how the Passports and Visas are supported in LifeScience AAI and available from LifeScience OpenID Connect (OIDC) Provider.

This presentation gives more information on the GA4GH Passports and Visas. A LifeScience ID (and also ELIXIR ID) holder can check their current Passport in this service: https://echo.aai.elixir-czech.org/

Relevant documents:

Instructions - Requesting GA4GH Passport and Visas in LS AAI

Instructions - integrating as GA4GH Passport and Visa source to LS AAI

Contents

Contexts

Context: LifeScience

- **ControlledAccessGrants** - none at the moment
- **AffiliationAndRole** - received from the user's Home Organisation's SAML Identity Provider, if available, or manually managed in the LS AAI (see), and affiliation within the LifeScience RI.
- **ResearcherStatus** - Derived from the AffiliationAndRole Visas.
- **LinkedIdentities** - derived from the LS AAI linked identities and the identifiers released by the user's Home Organisation's SAML Identity provider, if available, and derived from the ControlledAccessGrants Visas.
- **AcceptedTermsAndPolicies** - derived from an acceptance of terms and policies using the LS AAI group management functionality.

Context: ELIXIR

- **ControlledAccessGrants** - pulled from Visa Assertion Repositories external to ELIXIR (LS AAI)
    - Production sources
        - REMS SDS [CSC, Finland] (https://sd-apply.csc.fi/)
        - EGA [EGA, EMBL-EBI] (https://ega.ebi.ac.uk/)
        - REMS-BigPicture [CSC, Finland] (https://bp-rems.sd.csc.fi/)
        - REMS-UT-EE [University of Tartu, Estonia]
    - Testing sources:
        - EGAtest [EGA, EMBL-EBI] (https://ega.ebi.ac.uk:8053)
        - REMS-BigPictureDemo [CSC, Finland] (https://rems-bp-demo.rahtiapp.fi/)
- **AffiliationAndRole** - affiliation within ELIXIR.
- **ResearcherStatus** - derived from the AffiliationAndRole Visas.
- **LinkedIdentities** - derived from the ControlledAccessGrants Visas and ELIXIR ID.
- **AcceptedTermsAndPolicies** - derived from an acceptance of terms and policies using the LS AAI group management functionality.

AffiliationAndRole Visa

Context: LifeScience RI

Affiliation asserted by linking a Home Organization account to the LS AAI account

Description	The user's role within the identity's affiliated institution - e.g. faculty@cam.ac.uk - standard (eduPersonAffiliation) - e.g. nih.researcher@med.stanford.edu - proprietary (dot ".")
`Value *`	LS AAI populates this visa based on the external ID(s) the user has linked to their LS ID. - For Home Organisation logins (via eduGAIN) the value(s) is(are) the eduPersonScopedAffiliation attribute asserted by the Home Organisation IdP. - For commercial/community logins the value is *unknown* (e.g. unknown@google.com)
`Source *`	User's Home Organisation's URL (extracted from the Home Organisation IdP's OrganizationalURL SAML metadata element).
`Asserted *`	Timestamp from LS AAI when the Home Organization has last released this attribute (or when the linked commercial/community ID has last been used for login).
`Exp *`	One year after the *Asserted* timestamp.
`By`	*system*
`Conditions`	-
Notes	-

Example	{
	"sub": "3b466e0394068c5733247550e7240@lifescience-ri.eu",
	"ga4gh_visa_v1": {
	"asserted": 1662484240,
	"by": "system",
	"source": "https://www.muni.cz/en",
	"type": "AffiliationAndRole",
	"value": "employee@muni.cz"
	},
	"iss": "https://proxy.aai.lifescience-ri.eu/OIDC",
	"exp": 1694020240,
	"iat": 1662484243,
	"jti": "240681c2-e8cd-4aae-aa50-1116c11d64f1"
	}

Affiliation asserted manually by the organization's designated person in the LS AAI

Description	The user's role within an organization which has been manually granted by a designated person chosen by the organization with the tools in the LS AAI. This mechanism acts as a solution for home organizations, that cannot become a member of the eduGAIN or cannot release eduPersonScopedAffiliation as an attribute from their IdP - e.g. *faculty@organization.com*
`Value *`	A person can be granted affiliations: - *member@organization.domain.name* - and/or *affiliate@organization.domain.name*
`Source *`	Organisation's URL provided by the designated person is used. - e.g. *https://muni.cz/en*
`Asserted *`	The time when the user has been granted the affiliation value by the designated person.
`Exp *`	One year after the Asserted timestamp.
`By`	*so*
`Conditions`	-
Notes	For the management task details, see this document.

Example	{
	"sub": "3b466e0394068c5733247550e7240@lifescience-ri.eu",
	"ga4gh_visa_v1": {
	"asserted": 1662484240,
	"by": "so",
	"source": "https://www.muni.cz/en",
	"type": "AffiliationAndRole",
	"value": "member@muni.cz"
	},
	"iss": "https://proxy.aai.lifescience-ri.eu/OIDC",
	"exp": 1694020240,
	"iat": 1662484243,
	"jti": "a5a9ce71-3fbf-4777-a46c-10b2daf684fe"
	}

Affiliation within the Life Science RI

Description	The user's role within the LS AAI
`Value *`	Static values of *affiliate@lifescience-ri.eu* and *member@lifescience-ri.eu*.

Source *	https://lifescience-ri.eu/
Asserted *	Timestamp when the Visa has been issued
Exp *	Date of membership expiration in the LS AAI community group.
By	*system*
Conditions	-
Notes	-

Example	{
	  "sub": "3b466e0394068c5733247550e7240@lifescience-ri.eu",
	  "ga4gh_visa_v1": {
	  "asserted": 1570037082,
	  "by": "system",
	  "source": "https://lifescience-ri.eu/",
	  "type": "AffiliationAndRole",
	  "value": "member@cesnet.cz"
	  },
	  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC",
	  "exp": 1601659482,
	  "iat": 1582290933,
	  "jti": "73cb6736-04b4-4e4e-94f1-c9856ff342ac"
	}

Context: ELIXIR

Description	The user's affiliation with ELIXIR
`Value *`	ELIXIR populates this visa with a value *affiliate@elixir-europe.org.*
`Source *`	*https://www.elixir-europe.org/*
`Asserted *`	Timestamp when the Visa has been issued.
`Exp *`	One year after the Visa has been issued.
`By`	`system`
`Conditions`	-
Notes	-
Example	`{ "sub": "3b466e0394068c5733247550e7240@elixir-europe.org", "ga4gh_visa_v1": { "asserted": 1662484243, "by": "system", "source": "https://www.elixir-europe.org”, "type": "AffiliationAndRole", "value": "affiliate@elixir-europe.org" }, "iss": "https://proxy.aai.lifescience-ri.eu/OIDC", "exp": 1694020243, "iat": 1662484243, "jti": "4a86c86e-adf2-4c3b-8151-ea1292c7b0e6" }`

AcceptedTermsAndPolicies Visa

Context: LifeScience RI

Description	The Passport Visa Identity or the "source" organization has acknowledged the specific terms, policies, and conditions
`Value *`	*`https://doi.org/10.1038/s41431-018-0219-y`* (for registered access attestations)
`Source *`	*`https://lifescience-ri.eu/`*
`Asserted *`	Timestamp when the user made the registered access attestations.
`Exp *`	Timestamp when the Visa has been issued.
`By`	*`self`*
`Conditions`	-
Notes	-

Example	{
	  "sub": "3b466e0394068c5733247550e7240@lifescience-ri.eu",
	  "ga4gh_visa_v1": {
	  "asserted": 1559733029,
	  "by": "self",
	  "source": "https://lifescience-ri.eu/",
	  "type": "AcceptedTermsAndPolicies",
	  "value": "https://doi.org/10.1038/s41431-018-0219-y"
	  },
	  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC",
	  "exp": 4715406629,
	  "iat": 1582290933,
	  "jti": "7baa5f95-5acf-4433-a004-d4b79ce8ebc1"
	}

Context: ELIXIR

Description	The Passport Visa Identity or the "source" organization has acknowledged the specific terms, policies, and conditions
`Value *`	*`https://doi.org/10.1038/s41431-018-0219-y`* (for registered access attestations)
`Source *`	*`https://elixir-europe.org/`*
`Asserted *`	Timestamp when the Visa has been issued.
`Exp *`	100 years from the Asserted timestamp.
`By`	*`self`*
`Conditions`	-
Notes	See this slide for more information on AffiliationAndRole, ResearcherStatus, and AcceptedTermsAndPolicies in ELIXIR. More information on bona fide status is here. In ELIXIR, a user who qualifies for registered access can make the attestations here.

Example	`{`
	`  "sub": "3b466e0394068c5733247550e7240@elixir-europe.org",`
	`  "ga4gh_visa_v1": {`
	`  "asserted": 1559733029,`
	`  "by": "self",`
	`  "source": "https://elixir-europe.org/",`
	`  "type": "AcceptedTermsAndPolicies",`
	`  "value": "https://doi.org/10.1038/s41431-018-0219-y"`
	`  },`
	`  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC",`
	`  "exp": 4715406629,`
	`  "iat": 1582290933,`
	`  "jti": "7baa5f95-5acf-4433-a004-d4b79ce8ebc1"`
	`}`

ResearcherStatus Visa

Context: LifeScience RI

Description	The person has been acknowledged to be a researcher of a particular type or standard.
`Value *`	*`https://doi.org/10.1038/s41431-018-0219-y`* The value is asserted if 1. a user's Home Organisation IdP has released *`faculty`* affiliation (see AffliiationAndRole Visa), or 2. a user's Home Organisation's dedicated representative has manually elevated the user to *`faculty`* status in LS AAI, or 3. a peer who qualifies for any of the two above has vouched for the user's status as a bona fide researcher
`Source *`	*`https://lifescience-ri.eu/`*
`Asserted *`	Timestamp of when the user's researcher status has been asserted for the last time, using any of the alternatives 1-3 above.
`Exp *`	Alternative 1: 1 year after the Home Organisation asserted the affiliation Alternative 2: 1 year after the user has been granted the affiliation by the designated person Alternative 3: 1 year after the issuing of the visa
`By`	*`system`* (alternative 1) *`so`* (alternative 2) *`peer`* (alternative 3)
`Conditions`	-
Notes	-

Example	`{`
	`  "sub": "3b466e0394068c5733247550e7240@elixir-europe.org",`
	`  "ga4gh_visa_v1" : {`
	`  "asserted" : 1582290933,`
	`  "by" : "system",`
	`  "source" : "https://lifescience-ri.eu/",`
	`  "type" : "ResearcherStatus",`
	`  "value" : "https://doi.org/10.1038/s41431-018-0219-y"`
	`  },`
	`  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC",`
	`  "exp" : 1613913333,`
	`  "iat" : 1582290933,`
	`  "jti" : "fcaf42d3-47f3-42f8-bdcc-0b2724a05849"`
	`}`

Context: ELIXIR

Description	The person has been acknowledged to be a researcher of a particular type or standard.
`Value *`	*`https://doi.org/10.1038/s41431-018-0219-y`* The value is asserted if 1. a user's Home Organisation IdP has released *`faculty`* affiliation (see AffliiationAndRole Visa), or 2. a user's Home Organisation's dedicated representative has manually elevated the user to *`faculty`* status in LS AAI, or 3. a peer who qualifies for any of the two above has vouched for user's status as a bona fide researcher
`Source *`	*`https://elixir-europe.org/`*
`Asserted *`	Timestamp of when the user's researcher status has been asserted for the last time, using any of the alternatives 1-3 above.
`Exp *`	Alternative 1: 1 year after the Home Organisation asserted the affiliation Alternative 2: 1 year after the user has been granted the affiliation by the designated person Alternative 3: 1 year after the issuing of the visa
`By`	*`system`* (alternative 1) *`so`* (alternative 2) *`peer`* (alternative 3)
`Conditions`	-
Notes	See this slide for more information on AffiliationAndRole, ResearcherStatus, and AcceptedTermsAndPolicies in ELIXIR.

Example	`{`
	`  "sub": "3b466e0394068c5733247550e7240@elixir-europe.org",`
	`  "ga4gh_visa_v1" : {`
	`  "asserted" : 1582290933,`
	`  "by" : "so",`
	`  "source" : "https://elixir-europe.org/",`
	`  "type" : "ResearcherStatus",`
	`  "value" : "https://doi.org/10.1038/s41431-018-0219-y"`
	`  },`
	`  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC",`
	`  "exp" : 1613913333,`
	`  "iat" : 1582290933,`
	`  "jti" : "fcaf42d3-47f3-42f8-bdcc-0b2724a05849"`
	`}`

ControlledAccessGrants Visa

The ControlledAccessGrants Visas are not issued by the LS AAI OIDC server itself, they are taken from Embedded Token Issuers (as specified in the GA4GH Authentication and Authorization Infrastructure AAI OpenID Connect Profile specification) that digitally sign them so that the visas cannot be modified by subsequent Brokers like the LS AAI.

Context: LifeScience RI

Description	A dataset or other object for which controlled access has been granted to this Passport Visa Identity.
`Value *`	Identifier of the controlled access dataset, e.g. *`https://www.ebi.ac.uk/ega/datasets/EGAD00000000001`*
`Source *`	Identifier of the Data Access Committee who has approved the data access application, e.g. *`https://www.ebi.ac.uk/ega/dacs/EGAC00000000001`*
`Asserted *`	Timestamp of when the Data Access Committee has approved the data access application or timestamp from the Visa issuer for signing the visa.
`Exp *`	Expiration time asserted by the Data Access Committee.
`By`	*`dac`*
`Conditions`	Currently not asserted.
Notes	LifeScience currently supports ControlledAccessGrants issued by EGA and the REMS system. The Broker pulls the visas from their source any time a client (with the `ga4gh_passport_v1` scope) calls LifeScience Broker's */userinfo* endpoint. The visas are then cached for a short period of time (1 minute).
Example	`{ "sub": "a412f572d7b84823391beed05e8@lifescience-ri.eu", "ga4gh_visa_v1": { "type": "ControlledAccessGrants", "value": "https://www.ebi.ac.uk/ega/urn:hg:exa-contr", "source": "https://ga4gh.org/duri/no_org", "by": "dac", "asserted": 1568699331 }, "iss": "https://jwt-elixir-rems-proxy.rahtiapp.fi/", "iat": 1571809318, "exp": 1571812918, "jti": "950f9424-3452-446b-9a1c-da019fb497ec" }`

Context: ELIXIR

Description	A dataset or other object for which controlled access has been granted to this Passport Visa Identity.
`Value *`	Identifier of the controlled access dataset, e.g. *https://www.ebi.ac.uk/ega/datasets/EGAD00000000001*
`Source *`	Identifier of the Data Access Committee who has approved the data access application, e.g. *https://www.ebi.ac.uk/ega/dacs/EGAC00000000001*
`Asserted *`	Timestamp of when the Data Access Committee has approved the data access application or timestamp from the Visa issuer for signing the visa.
`Exp *`	Expiration time asserted by the Data Access Committee.
`By`	*dac*
`Conditions`	Currently not asserted.
Notes	LifeScience currently supports ControlledAccessGrants issued by EGA and the REMS system. The Broker pulls the visas from their source any time a client (with the `ga4gh_passport_v1` scope) calls LifeScience Broker's */userinfo* endpoint. The visas are then cached for a short period of time (1 minute).
Example	`{ "sub": "a412f572d7b84823391beed05e8@elixir-europe.org", "ga4gh_visa_v1": { "type": "ControlledAccessGrants", "value": "https://www.ebi.ac.uk/ega/urn:hg:exa-contr", "source": "https://ga4gh.org/duri/no_org", "by": "dac", "asserted": 1568699331 }, "iss": "https://jwt-elixir-rems-proxy.rahtiapp.fi/", "iat": 1571809318, "exp": 1571812918, "jti": "950f9424-3452-446b-9a1c-da019fb497ec" }`

LinkedIdentities Visa

Context: LifeScience RI

Description	The same person is often represented with different IDs (*“sub”*) by different visa issuers (*“iss”*) and the IDs are linked by ID linking services, such as LS AAI. The identity as indicated by the *{"sub", "iss"}* pair (aka. *"Passport Visa Identity"*) of the Passport Visa is the same as the identity or identities listed in the *"value"* field.
`Value *`	URL encoded *“sub”* and *“iss”* of the Passport Visa Identity, separated by *“,”*. For linked identities from SAML Home Organisation’s Identity Providers, the identifier (*eduPersonUniqueId*, *eduPersonPrincipalName*) and *SAML EntityID* of the Identity Provider (both values URL encoded), and separated with *“,”*. For social identity providers (Google, LinkedIn, ORCID, Apple, LS Username) the following values are used: - **ORCID:** *ORICD_ID,https://idhub.aai.lifescience-ri.eu/proxy/aHR0cHM6Ly9vcmNpZC5vcmcvb2F1dGgvYXV0aG9yaXpl* - **Google:** *Google_ID,https://idhub.aai.lifescience-ri.eu/proxy/aHR0cHM6Ly9hY2NvdW50cy5nb29nbGUuY29t* - **Apple:** *Apple_ID,https://idhub.aai.lifescience-ri.eu/proxy/aHR0cHM6Ly9hcHBsZWlkLmFwcGxlLmNvbQ==* - **LinkedIn:** *LinkedIn_ID,https://idhub.aai.lifescience-ri.eu/proxy/aHR0cHM6Ly93d3cubGlua2VkaW4uY29tL29hdXRoL3YyL2F1dGhvcml6YXRpb24=* - **LS Local Username&Password:** *LS_username@hostel.aai.lifescience-ri.eu,https://hostel.aai.lifescience-ri.eu/lshostel/* Also generates the identities using community identifiers (LifeScience ID, ELIXIR ID) in the following manner: - **LifeScience ID:** *LS_ID,https://proxy.aai.lifescience-ri.eu/proxy* - **ELIXIR ID:** *ELIXIR_ID,https://login.elixir-czech.org/idp/*
`Source *`	Identifier of service who did the ID linking. (at the moment, asserts by itself - *`https://lifescience-ri.eu/`*)

`Asserted *`	Timestamp of when the linked ID has been last used for logging in via AAI. In the case of community ID, the time when the Visa has been issued.
`Exp *`	1 year after the Asserted timestamp
`By`	*system*
`Conditions`	-
Notes	LS AAI currently asserts the LinkedIdentities Visa for the ID linking it has done by itself. The linked identities contain the identifiers released for the Home Organizations' accounts linked to the particular LS ID, as well as IDs used for querying the external Visa repositories if some Visa is returned.

Example	{
	  "sub": "a412f572d7b84823391beed05e8@lifescience-ri.eu",
	  "ga4gh_visa_v1": {
	  "asserted": 1582290963,
	  "by": "system",
	  "source": "https://lifescience-ri.eu/",
	  "type": "LinkedIdentities",
	  "value":
	"a412f572d7b84823391beed05e8%40elixir-europe.org,https%3A%2F%2Fjwt-elixir-rems-proxy.rahtiapp.fi%2F"
	  },
	  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC/",
	  "exp": 1613826963,
	  "iat": 1582290963,
	  "jti": "e73fff76-7f11-4b2c-bff4-27bbf31e63c6"
	}

Context: ELIXIR

Description	The same person is often represented with different IDs (*“sub”*) by different visa issuers (*“iss”*) and the IDs are linked by ID linking services, such as LS AAI. The identity as indicated by the *{"sub", "iss"}* pair (aka. *"Passport Visa Identity"*) of the Passport Visa is the same as the identity or identities listed in the *"value"* field.
`Value *`	URL encoded *“sub”* and *“iss”* of the Passport Visa Identity, separated by *“,”*.
`Source *`	Identifier of service who did the ID linking. (at the moment, asserts by itself - *`https://elixir-europe.org/`*)
`Asserted *`	Timestamp of when the ID linking was done.
`Exp *`	1 year after the Asserted timestamp
`By`	*`system`*
`Conditions`	-
Notes	Asserts the LinkedIdentities Visa for the ID linking it has done by itself.

Example	`{`
	`  "sub": "a412f572d7b84823391beed05e8@elixir-europe.org",`
	`  "ga4gh_visa_v1": {`
	`  "asserted": 1582290963,`
	`  "by": "system",`
	`  "source": "https://elixir-europe.org/",`
	`  "type": "LinkedIdentities",`
	`  "value":`
	`"a412f572d7b84823391beed05e8%40elixir-europe.org,https%3A%2F%2Fjwt-elixir-rems-proxy.rahtiapp.fi%2F"`
	`  },`
	`  "iss": "https://proxy.aai.lifescience-ri.eu/OIDC/",`
	`  "exp": 1613826963,`
	`  "iat": 1582290963,`
	`  "jti": "e73fff76-7f11-4b2c-bff4-27bbf31e63c6"`
	`}`