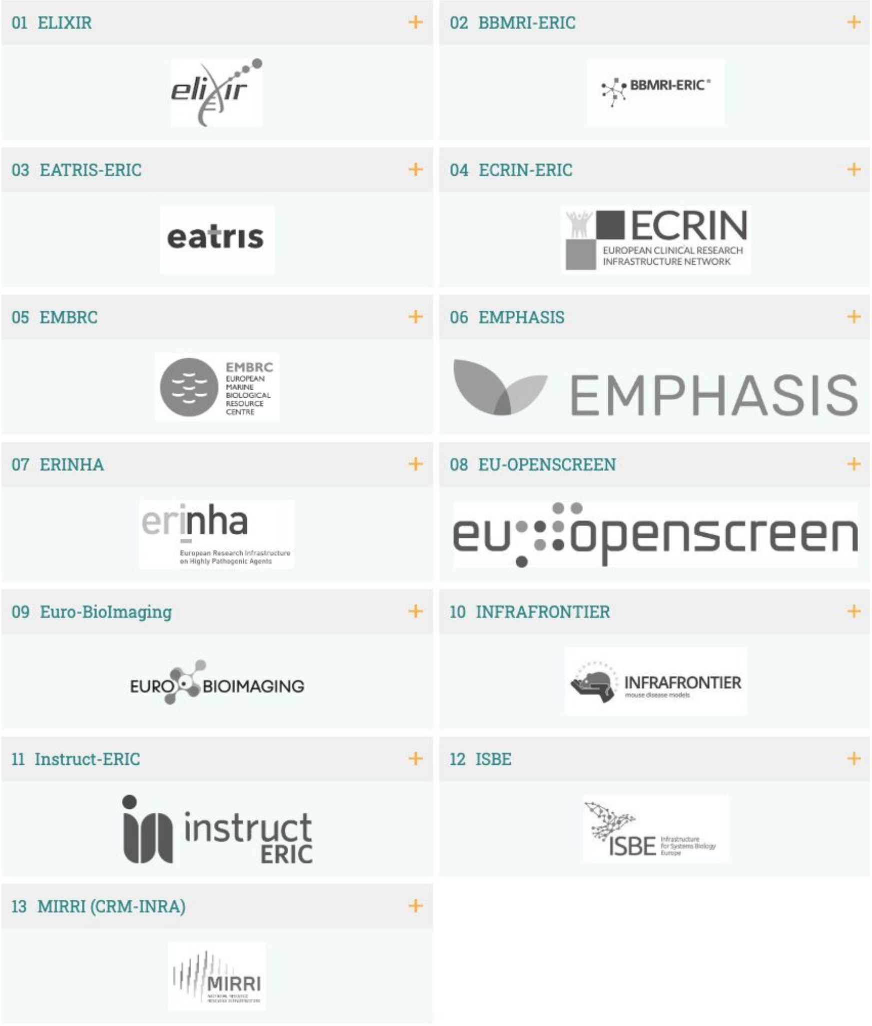
EOSC-Life
Life Sciences AAI

Pavel Břoušek
brousek@ics.muni.cz
MU/CESNET

EOSC-Life

EOSC-Life

- A consortium of 13 distributed research infrastructures and a total of 46 partners that connects a broad base of disciplines and links national research facilities and expert centres
- Variety of services and data available for the researchers
  - Including highly sensitive data



01 ELIXIR

02 BBMRI-ERIC

03 EATRIS-ERIC

04 ECRIN-ERIC

05 EMBRC

06 EMPHASIS

07 ERINHA

08 EU-OPENSCREEN

09 Euro-BioImaging

10 INFRAFRONTIER

11 Instruct-ERIC

12 ISBE

13 MIRRI (CRM-INRA)

+
elixir
BBMRI-ERIC
eatris
ECRIN
EUROPEAN CLINICAL RESEARCH INFRASTRUCTURE NETWORK
EMBRC
EUROPEAN MARINE BIOLOGICAL RESOURCE CENTRE
EMPHASIS
erinha
European Research Infrastructure on Highly Pathogenic Agents
eu-openscreen
EURO BIOIMAGING
INFRAFRONTIER
mouse disease models
instruct ERIC
ISBE
Infrastructure for Systems Biology Europe
MIRRI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824087

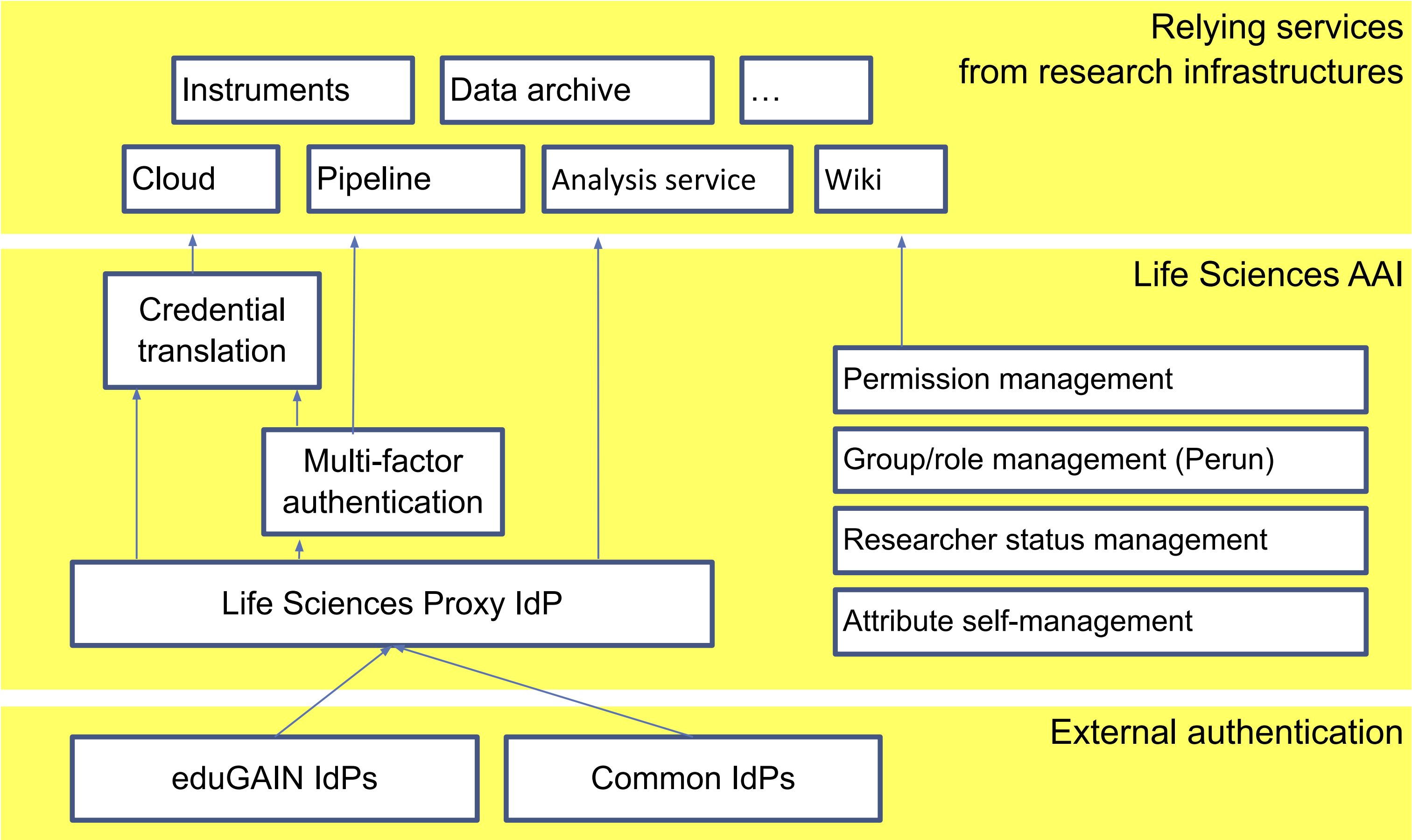
Life Sciences AAI

- To authenticate researchers and help the relying services manage their service access authorisation
- Requirements gathered in CORBEL WP5
- A pilot deployment in AARC2 project
- LS AAI blueprint published in August
  - https://doi.org/10.5281/zenodo.3386307
- EOSC-Life WP5 deploying into production
- Together with e-infrastructures (GEANT, EGI, CESNET)

WP5 Participant	**PM**
Masaryk University (ELIXIR-CZ)	40
Instruct	39
CSC - IT Center for Science (ELIXIR-FI)	38
INFRAFRONTIER	9
EuroBioImaging	9
BBMRI-ERIC	3
MIRRI	3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824087

Life Sciences AAI



Based on AARC Blueprint Architecture

Basic functionality set up

Sorting out policy matters

- GDPR

Key technologies

- Perun (IdM back-end)
- SATOSA (SAML2&OIDC proxy)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824087

Global Alliance
for Genomics & Health

Collaborate. Innovate. Accelerate.

Expressing researchers’ data access permissions

https://www.ga4gh.org/

Global Alliance
for Genomics & Health

Collaborate. Innovate. Accelerate.

The Global Alliance for Genomics and Health (GA4GH) is a policy-framing and technical standards-setting organization, seeking to enable responsible genomic data sharing within a human rights framework.

GA4GH Passports specification

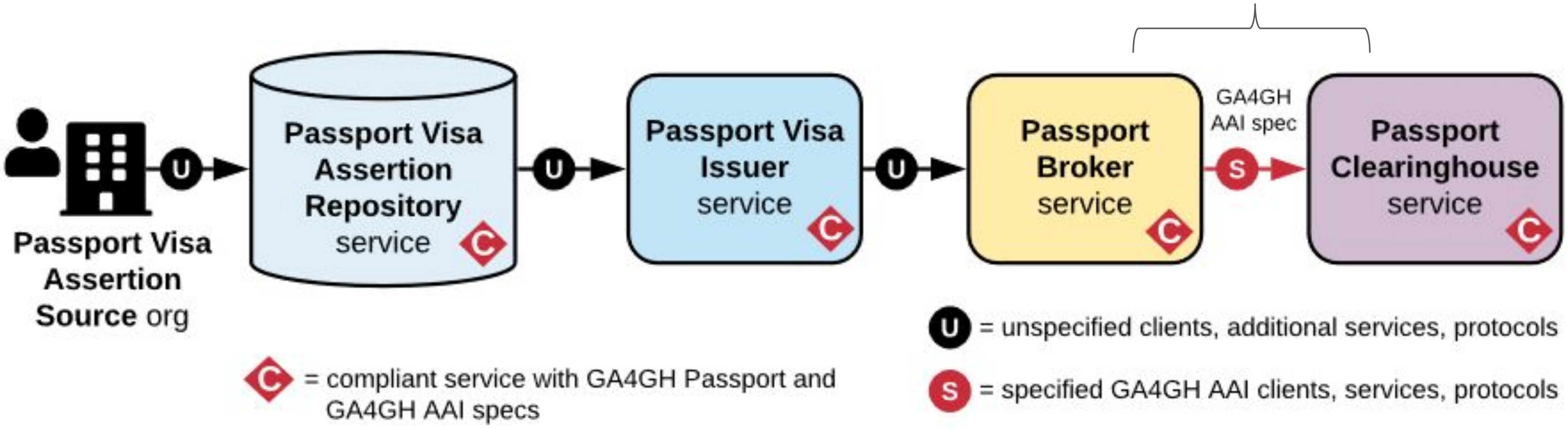
- **representation** of claims for registered and controlled access
- Approved 23 Oct 2019

GA4GH AAI OpenID Connect profile

- **protocol** for retrieving Passports from OIDC brokers
- Approved 23 Oct 2019

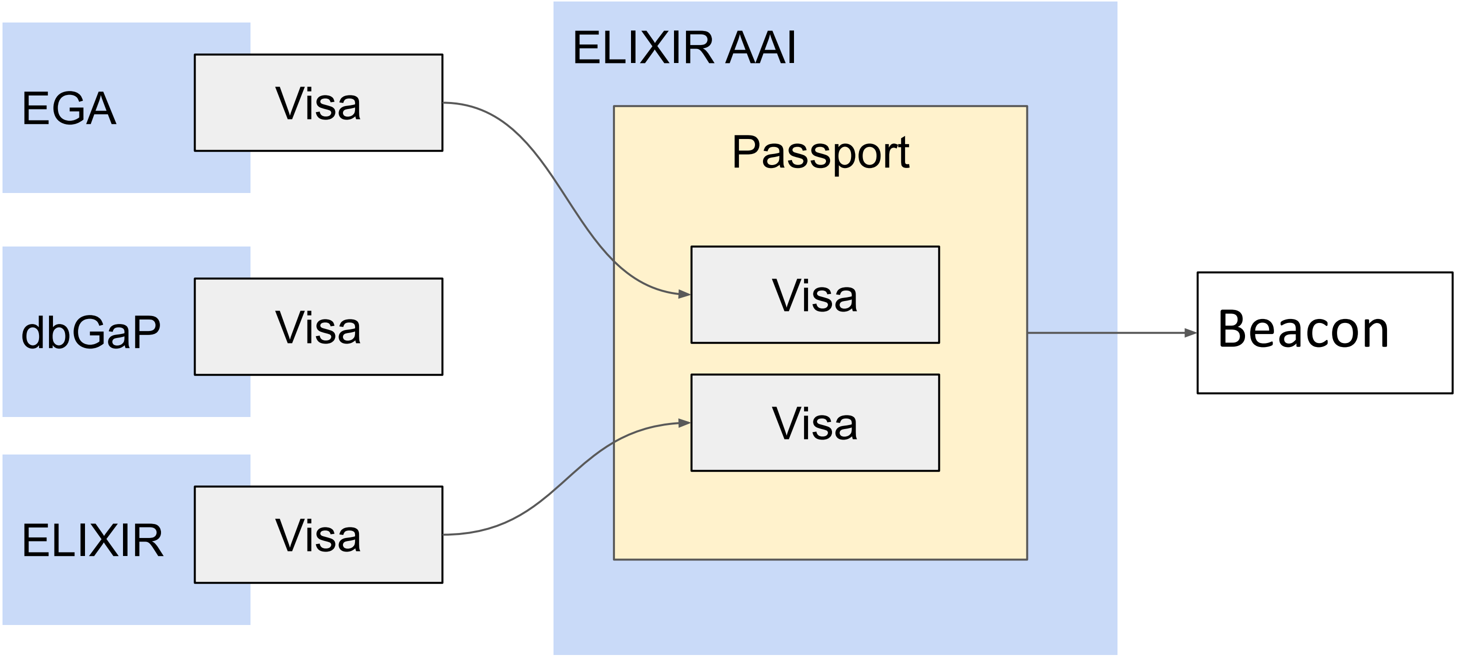
Passport actors

OIDC runs here


Passport Visa Assertion Source org
U
Passport Visa Assertion Repository service
C
U
Passport Visa Issuer service
C
U
Passport Broker service
C
GA4GH AAI spec
S
Passport Clearinghouse service
C
C = compliant service with GA4GH Passport and GA4GH AAI specs
U = unspecified clients, additional services, protocols
S = specified GA4GH AAI clients, services, protocols

There can be several Passport brokers in a chain.

Passport can have Visas from several sources



- A passport contains Visas from several sources
- Broker can decide which Visas to include
- Visas are JWT signed by their issuers

Visa assertion sources

Passport broker

Passport clearinghouse

Passport Visa types

AffiliationAndRole	The Passport Visa Identity'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 ".")
AcceptedTermsAndPolicies	The Passport Visa Identity or the "source" organization has **acknowledged the specific terms, policies, and conditions** - e.g. https://doi.org/10.1038/s41431-018-0219-y (registered access attestations)
ResearcherStatus	The person has been **acknowledged to be a researcher** of a particular type or standard. - e.g. https://doi.org/10.1038/s41431-018-0219-y (bona fide researcher for registered access)
ControlledAccessGrants	A **dataset** or other object for which **controlled access** has been granted to this Passport Visa Identity. - e.g. https://www.ebi.ac.uk/ega/datasets/EGAD00000000001
LinkedIdentities	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. - e.g. "mikael@elixir-europe.org equals to mlinden@csc.fi"

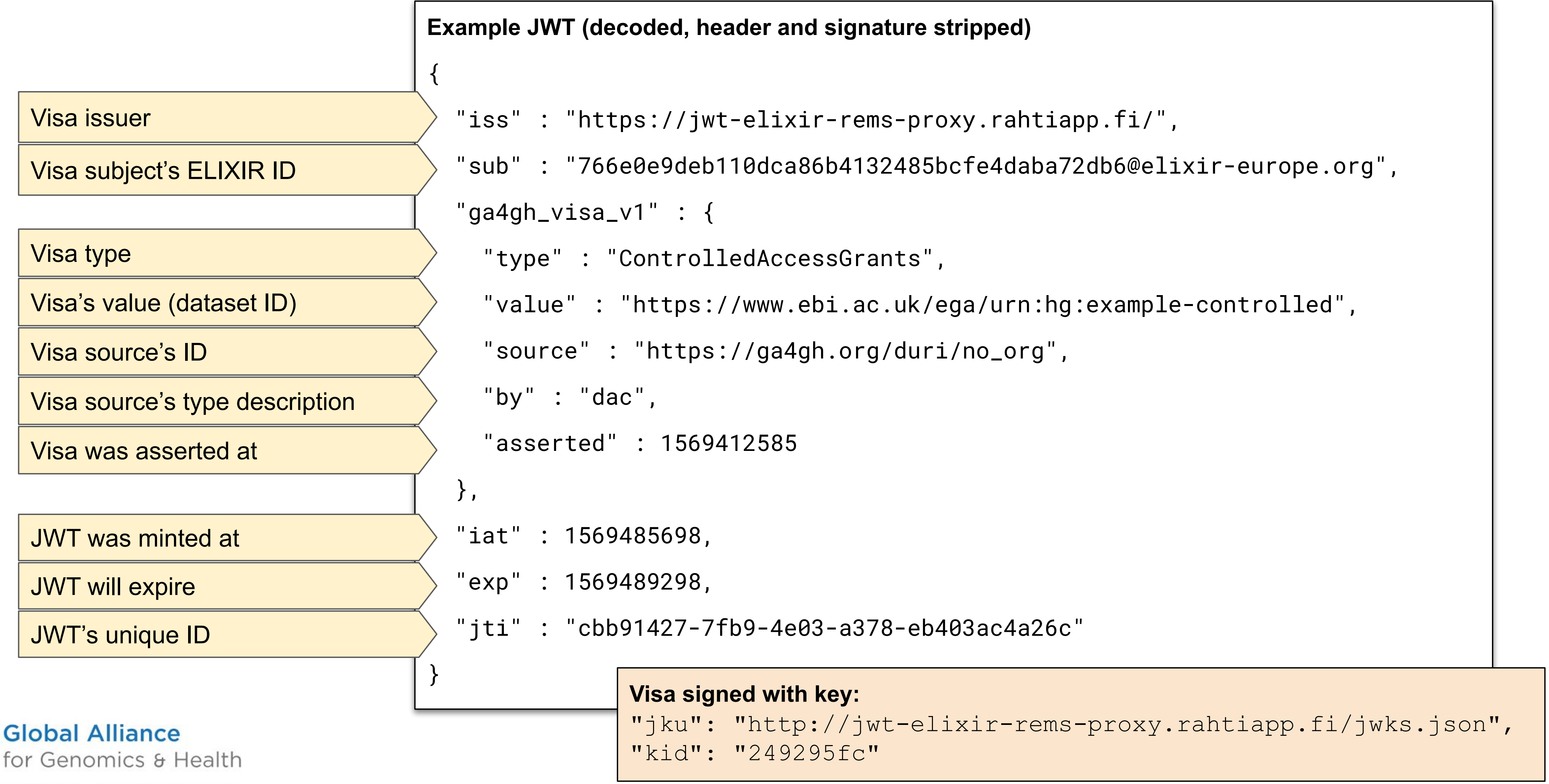
Registered access

Controlled access

Passport Visa fields

type *	Standard (see previous slide) or a custom **type of the Visa**
value *	URI **Value of the claim** - e.g. https://doi.org/10.1038/s41431-018-0219-y for the registered access attestation, as per SOM Dyke et al - e.g. https://ega-archive.org/datasets/EGAD00000000001 for controlled access grant
source *	A URL that provides at a minimum the **organization that made the assertion** - e.g. https://www.ebi.ac.uk/ega/dacs/EGAC00000000001 for the EGA DAC - e.g. https://grid.ac/institutes/grid.225360.0 for EMBL-EBI
asserted *	Seconds since unix epoch that represents when the Passport Visa Assertion **Source made the claim** - e.g. when did the DAC approve the data access application - not the same as `iat` (issued at) which indicates when the JWT was minted
by	The level or **type of authority within the "source"** organization of the assertion - vocabulary: `self, peer, system, so, dac`
conditions	Indicates that the Passport Visa is **only valid if** the clauses of the conditions match - e.g. “person still has affiliation `faculty@helsinki.fi`”

Example Passport Visa (ControlledAccessGrant)



Example JWT (decoded, header and signature stripped)

```
{
  "iss" : "https://jwt-elixir-rems-proxy.rahtiapp.fi/",
  "sub" : "766e0e9deb110dca86b4132485bcfe4daba72db6@elixir-europe.org",
  "ga4gh_visa_v1" : {
    "type" : "ControlledAccessGrants",
    "value" : "https://www.ebi.ac.uk/ega/urn:hg:example-controlled",
    "source" : "https://ga4gh.org/duri/no_org",
    "by" : "dac",
    "asserted" : 1569412585
  },
  "iat" : 1569485698,
  "exp" : 1569489298,
  "jti" : "cbb91427-7fb9-4e03-a378-eb403ac4a26c"
}
```

Visa issuer

Visa subject’s ELIXIR ID

Visa type

Visa’s value (dataset ID)

Visa source’s ID

Visa source’s type description

Visa was asserted at

JWT was minted at

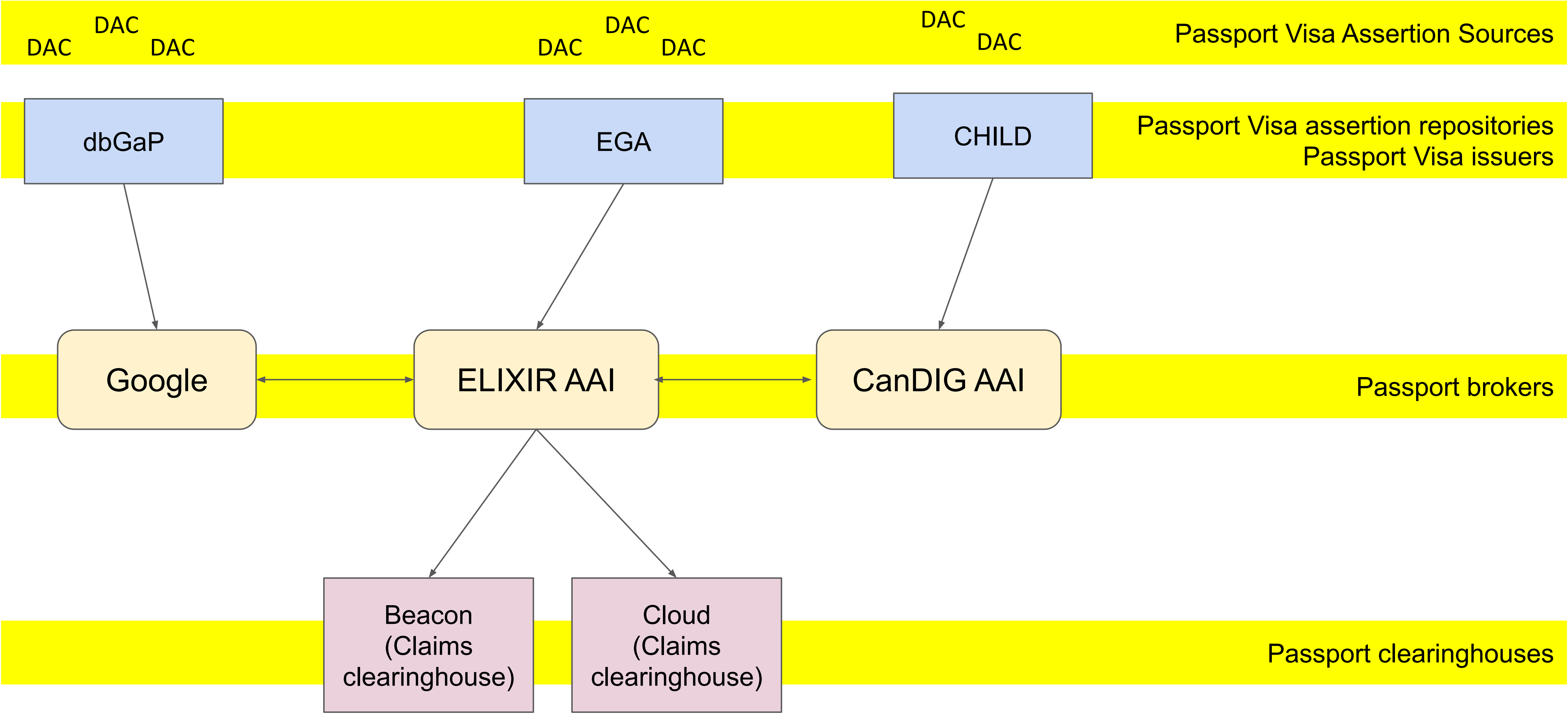
JWT will expire

JWT’s unique ID

Visa signed with key:

```
"jku": "http://jwt-elixir-rems-proxy.rahtiapp.fi/jwks.json",
"kid": "249295fc"
```

Example deployment


DAC
DAC
DAC
DAC
DAC
DAC
DAC
DAC
Passport Visa Assertion Sources
dbGaP
EGA
CHILD
Passport Visa assertion repositories
Passport Visa issuers
Google
ELIXIR AAI
CanDIG AAI
Passport brokers
Beacon (Claims clearinghouse)
Cloud (Claims clearinghouse)
Passport clearinghouses

Thank you

- https://www.ga4gh.org/