AARC project (Task NA3.1 “Level of Assurance”)

Level of Assurance survey for SP communities -- Summary of interviews

This document summarises the Level of Assurance interviews carried out among the research infrastructures. The document structure is based on the structured interview questions presented to the research and e-infrastructures.

Each infrastructure’s answers on the interview questions are presented in the table after the questions. In the last row of each table, the document also describes how the interview results have been reflected to the document “Recommendations on minimal assurance level relevant for low-risk research use cases”.

For more details on the method and the results, see the document “Recommendations on minimal assurance level relevant for low-risk research use cases”.

1.Introduction to LoA

Narrowly speaking, LoA for user authentication covers two things:

- Identity vetting: how an end user demonstrates his/her identity at the time when s/he receives the authentication credential from his/her Home Organisation (e.g. by presenting government photo-id face-to-face at a registration desk or self-registration on-line)
- authentication: how an end user proofs his/her identity to his/her Home Organisation's Identity Provider (IdP) server when s/he logs in (e.g. password or multi-factor authentication with a certificate or token)

More widely speaking, LoA can also cover e.g.

- management of credentials (e.g. delivery of credentials to their holder, revocation of credentials)
- information security management of the Home Organisation
- audits of the Home Organisation

Some people also count these in

- quality and freshness of user attributes (self-asserted by the user or Home Organisation vetted)
- Home Organisation's ability and willingness to populate and release the attributes to the SPs

2. Questions on the research infrastructures/communities

Who are your end users (who need to log in to your services):

- researchers with a Home Organisation (that operates or potentially operates an IdP)?
- citizen scientists?
- students with a Home Organisation (that operates or potentially operates an IdP)?
- else/what?

CLARIN	Researchers and students. For citizen scientists, CLARIN has its own guest IdP
DARIAH	Researchers, students and citizen scientists (less than 5%).
ELIXIR	Researchers, students and companies (up to 10% in some services)
photon/neutron	Researchers, students and industry (but they often have separate user management)
LIGO	Researchers, students, contractors in LIGO laboratories and some citizen scientists
EGI	Researchers, students, citizen scientists (via science gateways), private companies
PRACE	Researchers, students, industry users (small fraction)
WLGC	Researchers and students
Summary	End users are researchers, students (part of them have also the researcher role), citizen scientists (in some disciplines) and industry users (in some disciplines)
Reflection to the recommendation	No

If you are a research community

- is affiliation of a researcher (user) with your community typically longer lived than any organizational affiliation or employment, or does community membership stem primarily from organizational affiliation?

CLARIN	No, researchers affiliate well to their Home Organisations
DARIAH	Yes. Researchers' account in DARIAH stays if s/he changes his/her affiliation.

ELIXIR	No. Some are nomadic but access rights often cease when a researcher changes the HO.
photon/neutron	Yes. Users keep their identity (in Umbrella) when they change the affiliation
LIGO	Yes, there are nomadic users.
EGI	Common, depending on the user community (VO)
PRACE	N/A (PRACE is not a research community)
WLGC	Users are affiliated to their Home Organisation (via X.509 DNs)
Summary	Both practices do exist.
Reflection to the recommendation	No

- do you consider yourself also as a source of (identity) assurance for your community members?

CLARIN	No, see above
DARIAH	Yes
ELIXIR	Possible in the future (ELIXIR AAI)
photon/neutron	Yes, Umbrella system is the source of identity
LIGO	Yes, LIGO issues LIGO identities and operates an IdP for them
EGI	For some communities, there is a service (User Management Portal) that provides this kind of functionality
PRACE	N/A (PRACE is not a research community)
WLGC	Yes, via the VOMS service
Summary	Most research/e-infrastructures manage identities and attributes of their own for the end users. CLARIN is the notable exception.
Reflection to the recommendation	No

3.Questions on Identity and Authentication

User's "network identity" distinguishes him/her from other users of the SP.

3.1. Identity concept

How important is it for you that

- all user identities (accounts in the Home Organisation) belongs to an individual person (i.e. there are no shared accounts like "libraryuser1". Any robot/automated agent is traceable to a named person)?

CLARIN	Important
DARIAH	Important (non-personal accounts must at least be tagged)
ELIXIR	Important
photon/neutron	Important (in practice the facilities require personal accounts)
LIGO	Important
EGI	Mandatory
PRACE	Mandatory
WLGC	Important
Summary	All require that accounts belong to an individual user.
Reflection to the recommendation	Requirement 1

- and all users are traceable (i.e. the Home Organization knows who they are and can reach them)?

CLARIN	Important
DARIAH	Important
ELIXIR	Important
photon/neutron	Important (due to the regulatory obligations)
LIGO	Important
EGI	Mandatory

PRACE	Mandatory
WLGC	Important
Summary	All require that the Home Organisation knows who the end users are.
Reflection to the recommendation	Requirement 1

- and the Home Organisation is willing to collaborate with you if you think their user misbehaves in your service?

CLARIN	Moderately important (no experience on incidents)
DARIAH	Important
ELIXIR	Important (although can hardly enforce the HO to react)
photon/neutron	Not that important (instead, we will shut down a misbehaving user)
LIGO	Important (SIRTFI supported)
EGI	Important
PRACE	Mandatory (incidents, mostly)
WLGC	Important, Home Organisations must commit to WLGC's incident response policy
Summary	Most research/e-infrastructures require co-operation when a user misbehaves, although usually being able to exclude the user from the infrastructure is the primary reaction to misbehaviour.
Reflection to the recommendation	No. Possibly require Sirtfi in the later higher LoA level specification.

- that you (as an SP) can block him/her from your service?

CLARIN	Important
DARIAH	Important
ELIXIR	Important
photon/neutron	Important
LIGO	Important

EGI	Important
PRACE	Mandatory
WLGC	Important (the primary way)
Summary	All infrastructures consider this important.
Reflection to the recommendation	No

- user identifiers are persistent i.e. a user account is not re-assigned (re-cycled) to another person over time?

CLARIN	Important (both for accountability and authorisation)
DARIAH	Important (or at least must be able to detect re-assignment)
ELIXIR	Important (or at least must detect a re-assignment)
photon/neutron	Important (for confidentiality of users' files)
LIGO	Important (for user authorisation)
EGI	Important
PRACE	Mandatory
WLGC	Important (for confidentality of user's files)
Summary	Persistent, non-reassignable user identifiers are important for everyone.
Reflection to the recommendation	Requirement 2

- user identifiers are shared by multiple SPs i.e. if you have 2 SPs, do they both receive the same user identifier when the same user logs in to the two services?

CLARIN	Important (there are Attribute Provider scenarios)
DARIAH	Important (necessary to map the same user between multiple SPs)
ELIXIR	No (plan to introduce a centralised proxy)
photon/neutron	No (Umbrella is a proxy-based architecture)
LIGO	Important
EGI	Important

PRACE	Mandatory
WLGC	Important (X.509 DN used)
Summary	The infrastructures whose architecture is based on a proxy do not feel shared identifiers important.
Reflection to the recommendation	No

3.2.Initial proof of identity

How important is it for you that

- the Home Organization has a documented identity vetting process (whatever it is) in English and you can study it?

CLARIN	Important (we could look at it when a user from a new HO appears)
DARIAH	No (whatever is good enough for the Home Federation is good enough for DARIAH)
ELIXIR	Important
photon/neutron	Not important (project proposals are screened based on their scientific quality. F2F identity vetting is done when users come to a facility to do their experiment)
LIGO	Moderately important (we rely on a senior LIGO researcher in the Home Organisation to meet a new user face-to-face and confirm his/her ePPN anyway)
EGI	Important (science gateways are exception but have compensating controls)
PRACE	Mandatory (most importantly, the practice must be published)
WLGC	Important (face-to-face identity vetting needed)
Summary	Majority of the infrastructures consider Home Organisations' documented identity vetting procedures important. Some (photon/neutron and LIGO) do not count on it but have in place their own complementing infrastructure for identity vetting.
Reflection to the recommendation	Requirement 3

- each Home Organisation has a machine-readable tag that indicates how the organization carries out identity proofing and the tag is from a well-defined international vocabulary?

CLARIN	Could make life easier (e.g. trigger manual check of HO). Clarin has hundreds of potential HOs
DARIAH	No (see above)
ELIXIR	Yes, would reduce manual checks
photon/neutron	No (see above)
LIGO	No (see above)
EGI	Desirable (the IGTF certificate could then be issued to match the tag)
PRACE	Desirable (e.g. relying on IGTF profiles)
WLGC	Important (face-to-face identity vetting needed)
Summary	The more the infrastructure relies on Home Organisations' identity vetting procedures the more they desire useful tags for it.
Reflection to the recommendation	Implementation note.

- each user in a Home Organisation has the above tag and different end users in the same organization can have different tags (depending how their identity was initially proofed)?

CLARIN	Its OK.
DARIAH	No (see above)
ELIXIR	Sounds reasonable (tags need standardisation of course)
photon/neutron	No (see above)
LIGO	No (see above)
EGI	Desirable
PRACE	Desirable, there may be use cases
WLGC	Yes (if needed for face-to-face identity vetting)
Summary	The more the infrastructure relies on Home Organisations' identity vetting procedures the more they desire useful tags for it.
Reflection to the recommendation	Implementation note.

- the identity proofing is done face-to-face based on a government photo-ID or equivalent?

CLARIN	Currently just few that sensitive services that they needed it but they are coming
DARIAH	Not important.
ELIXIR	For some services yes
photon/neutron	Currently, no
LIGO	No (see above)
EGI	Depends on the service. IGTF profiles BIRCH (MICS) and CEDAR (classic) require it.
PRACE	Not mandatory (won't always be possible)
WLGC	Important
Summary	For those infrastructures who rely on Home Organisations' identity vetting procedures, ELIXIR, EGI and WLGC feel it important. Some infrastructures (photon/neutron and LIGO) have in place their own complementing infrastructure for face to face identity vetting.
Reflection to the recommendation	No. Possibly take into account in the later higher LoA level specification.

3.3.On-line authentication

- Are password-based authentication good enough for you?

CLARIN	Yes, for now
DARIAH	Yes
ELIXIR	Yes, for less sensitive services
photon/neutron	Yes
LIGO	Yes, for most of the services
EGI	Yes, de facto
PRACE	Yes
WLGC	Yes, for less sensitive services
Summary	Passwords are widely accepted at least for less sensitive services.

Reflection to the recommendation	Requirement 4

- Should passwords have some kind of quality floor? (What kind of quality floor?)

CLARIN	Would be nice
DARIAH	No (whatever is good enough for the national federation is good enough for DARIAH)
ELIXIR	Yes, it’s a common practice in the Internet
photon/neutron	Yes, normal requirements on complexity, length, etc…
LIGO	Yes, we run password cracking software when new passwords are set
EGI	Yes, length and complexity
PRACE	Yes, length and complexity
WLGC	Yes, minimum complexity would be good.
Summary	Most research infrastructures expect some complexity baseline for passwords.
Reflection to the recommendation	Requirement 4

- Do you need two factor authentication? (What kind of?) Are you willing to share its costs?

CLARIN	Currently just few that sensitive services, but they are coming. Unsure about cost sharing.
DARIAH	No
ELIXIR	For sensitive services, yes. ELIXIR is willing to pay for it.
photon/neutron	Some facilities are considering buying a product for 2FA (so, yes)
LIGO	Yes, for more sensitive services
EGI	Currently no requests from user communities
PRACE	Preferably (currently use IGTF certificates). No cost contribution.
WLGC	Yes, for some services (like job submission)
Summary	Some infrastructures have a need for two factor authentication for the more sensitive services. Only one is willing to pay for it.

Reflection to the recommendation	No. Possibly take into account in the later higher LoA level specification.

3.4.Step-up authentication as a service

Step-up authentication means that the user first authenticates with a password, and subsequently with a second factor (such as by a one-time password delivered to his/her cellphone). Step-up authentication could be delivered to research communities as a service.
Would you like to make use of step-up authentication

- if it costs you money?
- if it costs you work (for instance, you need to operate one or several registration authorities where your community's users come to show their photo-ID and you record their cellphone number)?

CLARIN	Not for now
DARIAH	No
ELIXIR	Yes, ELIXIR can pay for it. Preferred approach is that e.g. GEANT operates the service. Global coverage needed.
photon/neutron	Some facilities could pay for step-up authentication
LIGO	LIGO could use step-up authentication if it was available and costs not too much.
EGI	Some user communities may want it and pay for it. EGI is already used to the PKI model (with registration authorities)
PRACE	No cost contribution. Currently using the IGTF certificates (which do not cost us)
WLGC	Not known (depends on the use case)
Summary	ELIXIR, LIGO and possibly some photon/neutron and EGI communities could be interested.
Reflection to the recommendation	No

4. Questions on user attributes

Besides an identifier, the Home Organisation's Identity Provider is able to deliver also other attributes of the person that logs in.

4.1. Freshness of user accounts and attributes

Many Home Organisations close the user account when an individual departs (e.g. researcher changes his/her employer). Closing the account closes also federated access to your SP. However, some organisations keep the accounts open (e.g. to serve alumni etc).

- Do you expect that user accounts are closed as a user departs? How promptly?
- Do you expect that user's role attributes (e.g. eduPersonAffiliation="faculty") value is updated as an individual departs? How promptly?

CLARIN	Promply, within a week
DARIAH	Account closure in 90 days after departure is enough. No use for ePA.
ELIXIR	Important, within a month
photon/neutron	No, Umbrella doesn’t make use of that information
LIGO	No, LIGO does not make use of that information but manages departing users with its internal procedures
EGI	Yes but there are also other controls available for the user communities (VOMS, User Management Portal)
PRACE	Yes, immediatelly (the day s/he leaves the organisation)
WLGC	Desirable within one year (there are also other controls like VOMS)
Summary	The infrastructures (photon/neutron, LIGO, EGI, WLGC) who do not count on Home Organisation released attributes have no requirements on the freshness of user attributes, or the requirements are relaxed (e.g. account closure in one year). Those infrastructures who count more on Home Organisations’ attributes would like to see the account to be closed or ePA to be updated within 1-90 days of the user’s departure.
Reflection to the recommendation	Requirement 5

4.2. Quality/provenance of user data

In larger universities the IdP/IdM gathers users' attributes from several registries (payroll system, CRIS (current research information system), student registry) with varying data quality. Some attributes can even be self-asserted by the user him/herself.

- Is it important for you to know the quality/provenance of the user data on the attribute level? What attributes? On what level of granularity?

CLARIN	displayname, cn, eppn, ePTID and schacHomeOrganisation and schacHomeOrganisationtype should not be self-asserted.
DARIAH	Currently no. It would be good to receive a reliable value for email.
ELIXIR	For people with strong identity vetting. eduPersonAffiliation, common name, (sometimes the phone number), unique ID, assurance level
photon/neutron	Currently no. However, there is a plan to start to make use of that information, then attribute-level provenance gets interesting
LIGO	No strong requirements
EGI	Important. Contact attributes: email and phone (self-asserted is enough)
PRACE	Important. Contact attributes: email and phone (self-asserted is enough)
WLGC	No (WLGC does not rely on HO released attributes for authorisation)
Summary	There are infrastructures who do not count on the attributes released by the Home Organisation but use the Home Organisation mostly just as an authenticaton provider (DARIAH, photon/neutron, LIGO, WLGC). For the other infrastructures, unique identifier (ePPN/ePTID), name, e-mail address and phone number were the most frequent attributes.
Reflection to the recommendation	No

4.3. Population and release of attributes

- What are the key attributes Home Organisations should populate for their end users and release to your SP?

CLARIN	displayname, cn, eppn, ePTID and schacHomeOrganisation, schacHomeOrganisationtype. Currently release of attributes is even more important than LoA.
DARIAH	ePPN, e-mail, displayName and o
ELIXIR	name and unique identifier
photon/neutron	SAML2 Persistent ID/eduPersonTargetedID
LIGO	unique ID (ePPN/ePTID). Possibly some interest in e-mail address and cn.
EGI	Required: { givenName and sn (Surname) } or {commonName}

	eduPersonUniqueID or a non-re-assigned eduPersonPrincipalName (not eduPersonTargetedID because it can be different for different SPs)
PRACE	givenName, sn, mail, telephoneNumber, schacPersonalTitle, schacCountryofCitizenship, eduPersonPrincipalName
WLGC	Non-reassignable unique ID, full name and email address
Summary	The most frequently requested attributes were unique ID (ePPN or ePTID), full name, and e-mail address
Reflection to the recommendation	No

5.Questions on audits

- Is it enough for you that a Home Organisation self-asserts that it complies with a certain LoA level?
- Should some external body have some enforcement rights (e.g. Home identity federation can remove “compliant” tag from the Home Organisation if there are doubts that a Home Organisation fails its LoA level)?
- Are internal periodic self-assessments needed? Should these be reviewed (or open to review) by e.g. the Home identity federation or federation peers?
- Are internal audits needed where the auditors are from an independent organization unit?

CLARIN	Periodic self-assessment are a good start but the requirements must be transparent.
DARIAH	Whatever is enough for the national federation is enough for DARIAH, too.
ELIXIR	Periodic self-assessment.
photon/neutron	Periodic self-assessment. Some kind of monitoring if a HO has gone wild would be good.
LIGO	Whatever is enough for the Home Organisation’s internal needs is enough for LIGO.
EGI	Self-evaluation based on specific and comprehensive requirements, with 1-3 year peer review cycle. Organisation’s high-level practices should be published.
PRACE	Self-assertion based on specific and comprehensive requirements, not just identity vetting and authentication but also information security more widely. Negative self-evaluation should lead to exclusion.
WLGC	For minimum LoA level, self-assessment based on comprehensive enough requirements. For higher assurance, peer assessment preferred.

Summary	The majority of infrastructures proposed periodic self-assessments made based on requirements that are comprehensive enough.
Reflection to the recommendation	Requirement 6

- Are external audits needed? Are you willing to share their costs?

CLARIN	Currently not willing to share costs
DARIAH	No
ELIXIR	Sharing costs difficult because many HOs
photon/neutron	External audit would be too expensive
LIGO	No
EGI	EGI does not insist on external audits and has no interest in sharing costs.
PRACE	Would be nice but no cost contribution.
WLGC	No, unnecessarily expensive
Summary	External audits were considered too expensive
Reflection to the recommendation	No. Possibly take into account in the later higher LoA level specification.