Survey development area

2.1. A. Generic

1. Which Research Infrastructure (RI) are you representing?
2. Which field of science are you serving? (Frascati manual of Fields of Research and Development (FORD)) (can we compile a list?)
3. Please provide description about the research infrastructure (e.g. which kind of infrastructure and related services are delivered and by whom, is there a formalised collaboration etc.)
4. Please provide description of the user audience - type of users (research, citizen scientists, industry users), number of users, distribution over the globe and organisations
5. Is the RI member of European Open Science Cloud (EOSC)?
6. Is the RI participating in Citizen Science Programmes or other initiatives or programmes?

2.2. B. AAI solution

(probably 2 sets of question based on the BPA knowledge level - BPA beginner/rookie vs BPA savvy/advanced user)

1. Describe the currently running solution for authentication and authorisation infrastructure (AAI). (Which specific authentication methods being used to cater for different user audience (e.g Institutional accounts (eduGAIN), ORCID, Social media, Others - please specify))
2. Is your AAI solution compliant to AARC BPA (blueprint architecture)?
3. Which AARC guidelines are you implementing? (add the table...)
4. What is your comments about BPA implementation? (challenges in implementation, challenges in clarity, technical difficulties etc.)

(introduction material needed to present BPA and the guidelines)

- YES / NO - Guidelines for expressing community user identifiers (AARC-G026)
- YES / NO - Guidelines on expressing group membership and role information (AARC-G002) (superseded by AARC-G069)
- YES / NO - Guidelines on expressing group membership and role information (AARC-G069)
- YES / NO - Specification for expressing resource capabilities (AARC-G027)
- YES / NO - Guidelines for expressing affiliation information (AARC-G025)
- YES / NO - Inference and constructing voPersonExternalAffiliation (AARC-G057)
- YES / NO - Exchange of specific assurance information between Infrastructure (AARC-G021)
- YES / NO - Guidelines for evaluating the combined assurance of linked identities (AARC-G031)
- YES / NO - A specification for IdP hinting (AARC-G049) (superseded by AARC-G061)
- YES / NO - A specification for IdP hinting (AARC-G061)
- YES / NO - Specification for hinting an IdP which discovery service to use (AARC-G062)
- YES / NO - A specification for providing information about an end service (AARC-G063)
- YES / NO - Guidelines for Secure Operation of Attribute Authorities (AARC-G071)

2.3. C. Policy for access management

1. Does the Research Infrastructures have an access policy? (the access policy governs who can access the infrastructure, under what conditions)
2. Is there a formalised procedure to manage access rights to services (e.g. cooperation agreement, call for application and evaluation, ad-hoc individual order/access, member of an organisation, etc.)?
3. How do you implement the policy for access management (e.g. how is the individual who can access the research research data/measurement data/your research instrument identified and authorised)?
   - Please select any of the following options that apply (try first without asking the list)
     - (a) Based on the user’s membership in group(s). If YES, do these groups need to be managed within your RI or within external RIs?
     - (b) Based on user attributes required to access specific resources a user is allowed to access or perform certain actions. If YES, do these capabilities need to be managed within your RI or within external RIs? - ask Nicolas for the example? e.g ESI?
     - (c) Based on affiliation of the user with their home institute
     - (d) Based on identity assurance (e.g. level of identity proofing, freshness of affiliation information),
     - (e) Based on the authentication method (e.g. Multi-Factor Authentication - MFA),
     - (f) Other
4. What are the requirements for identification of the users (e.g. required information, LoA, authentication method)?
   - Please select any of the following options that apply:
     - a) Globally unique persistent identifier,
     - b) Name (First / Last name),
     - c) Email,
     - d) Affiliation with the home institute,
     - e) Identity assurance (e.g. level of identity proofing, freshness of affiliation information),
     - f) Authentication method (e.g. Multi-Factor Authentication - MFA),
     - g) Other

2.4. D. Workflow

1. Can you describe the research workflows?
Would it help to provide options for the service types? E.g. Please select the most appropriate service types for services in your RI:

- **Browser Accessible Service**: A service that provides a web interface that can be accessed by users using their browsers (e.g. A research data visualisation tool accessible through a web browser).

- **API Consumed by or on behalf of Users**: A service that provides an API that can be consumed programmatically by the end users or by other services using user-delegated credentials. (e.g. A data analysis API allowing researchers to programmatically retrieve and analyse datasets).

- **API Consumed by Services**: A service that provides an API to be consumed by other services. These services do not act on behalf of the user but have their own access rights to the API (e.g. A workflow management system might offer an API for other services to submit data jobs, monitor progress, and retrieve results.).

- **Client consuming Service APIs using delegated user identities**: A client that uses access tokens authorised/delegated by end users and which can use these access tokens to access “APIs Consumed by or on behalf of Users” (e.g. A research collaboration platform might offer an API for data analysis tools. Researchers can authorise these tools to access their research data stored on the platform using delegated access tokens).

- **Client consuming other Service APIs using its own client identity**: A client that uses its own identity and access token to access “APIs Consumed by Services” (e.g. A tool accessing a storage service API using its own client credentials to transfer data).

- **Public Access**: A service that does not require users to be authenticated and authorised before they can access its resources (e.g. A public dataset repository where anyone can access datasets without needing to log in). - two sides to this question: on ingress of data into a data source, and on egress, which may be un-authenticated. Does your infra need to distinguish between these two cases?

Based on the workflow we could ask sub-questions such as:

- Are the research data and databases of the Research Infrastructure accessible
  - yes, they are continuously accessible both inside and outside the institution
  - yes, they are continuously accessible from within the institution
  - Accessible to others on a case-by-case basis
  - Not accessible to others

- During the access of the Research Infrastructure which method is used (more than one option can be marked):
  - Providing measurement/database access based on research collaboration
  - Provision of measurement/database access for based on a contract
  - Measurements/database access with customer/requester access
  - Taking measurements/database access by providing online/remote access
  - Measurements/database access with data processing and evaluation
  - Other: (describe)

We could consider the following questions to understand if their AAI acts as a Community AAI, Infrastructure Proxy or both (alternatively these questions could be moved to Section B - AAI solution):

- Do users of your Research Infrastructure access services provided by other Infrastructures using your AAI? If yes, can you describe? (Please also mention your future plans in this area)
- Do users of other infrastructures access services provided by your Research Infrastructure using your AAI? If yes, can you describe? (Please also mention your future plans in this area.)

2.5. E. Requirements

(collect generic answers via E.1 question, then discuss in details with E.2 questions ad guideline)

1. Can you describe further requirements, gaps and challenges?
2. As we collect the answers, we will try to identify common requirements. We can use the EOSC AAI requirements as basis for this:

- **Stronger Authentication Methods**: Is the requirement to have stronger authentication methods in general, or is it specifically for accessing sensitive data? Stronger authentication methods could be employed to support the requirement for access to sensitive data.
- **Support for EU Digital Identity Wallets (EUDI Wallet)** — needs explanation/short presentation what purpose it can be used for.
- **Better user experience for authentication process**
- **Scalable solution limiting the number of consent requests in compliance with the GDPR**
- **Develop a policy requiring the community participants to provide a centralised point for managing data release decisions**
- **Scalable authorization model in EOSC AAI - also requires explanation**
- **Identity Vetting**

What about Policy related questions, e.g.:

- **Is there a GDPR Data Controller designated for the AAI?**
- **Has the AAI designated a security contact to handle security incidents?**
- **Does the AAI adhere to SIRTFI or other recognised security frameworks?**