Fed2 Survey or Interview Questions for Information Gathering

DRAFT

The purpose of this document it to record questions that will help us gather information about what Fed2 will need to look like. Asking our members what works for them and what doesn't, understand what their future needs might be or what they're not able to do currently.

End-User ~~(Researcher)~~ **Questions:**
- ~~Do you collaborate with others in your work/research?~~
- In what ways do you collaborate with remote peers?
  - With how many people?
  - Where are they situated?
  - Do you see/know (all) those people offline? How often do you see them?
- What types of online resources do you use to accomplish your goals?
  - Collaboration site (e.g. wiki, virtual organization, etc.)
  - Research libraries/collections
  - Shared applications
  - Research institutions/organizations
  - Data sets (better way to reference access to large data sets?)
  - Other?
- What obstacles do you encounter when collaborating with others using online resources?
- What resources are easy to access (and why)?
- In what situations do you need to reliably validate the identit(y)(ies) of those you collaborate with?
  - How do you currently do that?
  - How would you ideally do that, if anything goes? (Or maybe, "how do you wish you could do that?")
  - What type of information do you require from the other(s) in this context? (E.g. name, email address, role, …?)
- Are you able to replace all your online accounts that you use for work/research with just 1? If not, why (not)?
  - Would you want that? Why (not)?

Commented [1]: Inter-institutional research projects have to some extent driven federated identity requirements; that' been useful as new requirements are formulated and tested by motivated savvy folks, and implementation then raises value for everyone. So keep soliciting needs and new requirements from this sector, but also from the much larger community of scholars, teachers, and students whose sophistication might lag, but whose unique requirements might also enhance conceptions of FFED2. I.E., don't focus solely on "researcher" needs; as phrased, the majority of our users may think this question does not apply to them.

Commented [2]: Good point David. I'll remove the qualifier after we discuss (so your comment isn't lost).

Commented [3]: Maybe just "peers", and then one of the sub questions is near vs remote peers... (i.e., in the future, the line between near and remote may be more blurred...)

Commented [4]: Gets to the question of remote or local...

Commented [5]: Cloud Storage Services (e.g. Box, Google, etc) ... Private/Smart links very common with these types of services

Commented [6]: By "private/smart links", are you referring to using a link rather than a login to access a file or folder? Is there something about links that perhaps should be reflected in these questions? Eg, easy to share with a user lacking a federated identity; easier to use than typing in a password.

- - Where do you think you should get this single account (who should provide it?) Would you trust your institution to provide it? Why, or why not?
  - Is there any account that can (almost) do this today? If so, what is it? What are its shortcomings, if any?
- Do you currently use a product that "seems" to provide access to ALL the online resources you need to do your job, research, etc.?
  - If yes, what do you use?
  - What shortcomings, if any, would you like to see improved?
- Do you trust your institution to handle your identity information? If not, what is needed in order for you to trust that it protects your information and shares it only with tools and services that are trustable?
  - Is this level of trust important to you?
- Do you trust the services, applications, tools, and people you collaborate with to be good stewards of your identity information? Do they meet your expectations for the privacy of you name, email, account information, *etc*? If not, what do you need from them to earn that trust?
  - Is this type of trust important to you?
- If you were to write a novel that takes place in the future, what might be a surprising way that the characters might communicate with each other? How might research be conducted that is different from that today? How would the characters identify themselves in casual situations, in official situations, and in professional situations?
- Imagining [N years] in the future, would you want to access institutional and research resources via a voice assistant such as Siri or Alexa or some similar tool?
- Imagining [N years] in the future, would you want to access resources with agents or bots or unattended applications on your behalf?
- Imagining [N years] in the future, how would you like to be able to use your R&E/academic identity? What parts of that identity would you want to control and what parts would you like your home institution to assert? Are there agencies or other organizations that contain assertions that you would like included as part of your identity?

Organizational Questions (University, 2-yr HE/FE, Research Organization):
- Thinking 5/10/15 years out, what are the major challenges/opportunities that you expect will impact your organization's ability to collaborate with your peers?
  - Technology
    - Major cloud infrastructure / service

Commented [7]: Looking for a way to capture "competition" to Federation, SAML, solutions which may whittle away at our community base (or prevent growth)

Commented [8]: I tried to capture this in the previous question...

Deleted: do you need to

Deleted: What assurances do you need from the relying parties?...

Commented [11]: Is this question (and the 3 below) one we would ask on a survey or during an interview, or one we might ask ourselves once we have gathered data from others? (Maybe too early to ask this.)

Commented [12]: It's not uncommon for something like this to be on a survey (often phrased as an "oracle" question), mainly because it is often easier to get a broad reach and a greater diversity of lenses and perspectives to help stretch thinking.

Commented [13]: Proposed questions for pushing the future boundary (need less technical framing)

Commented [14]: Some of these things I feel like I should be able to do today. I've also found it difficult to get people to think about what they will be doing in the future.

It may be better to talk about the future boundary in terms of more general terms: "If you were to write a novel that takes place in the future, what might be a surprising way to communicate | model for conducting research | identify yourself that would be in your book?"

Commented [15]: Although not specifically mentioned I assume these questions are for the people responsible for IdM within their organization. If not the questions I've added do not make a lot of sense ;-)

Commented [16]: Yes. While they may not be doing federation (yet) they at least have to have some type of Identity Management in place to answer the questions.

- - - IoT / smart, autonomous agents
    - Cybersecurity threats (is this technology?)
  - Legal/Policy
  - Social attitude toward privacy/information sharing
  - Political?
  - Novel collaboration scenarios (beyond traditional research), e.g., intellectual property consortium; industry collaborations;
- Do you have a Single Sign-On (SSO) solution for your organization? Why (not)?
  - If yes: do you need additional solutions for edge use cases? (I.e. what is not covered by this SSO solution?)
- If you could outsource anything related to Identity Management (IdM), SSO, … what would it be? Why?
  - Or the other way around, if too much is already outsourced ;-)
- Do you ever hear complaints from within your organisation about IdM/SSO? What/why?
- What do you think about the rise of consolidated identities (i.e. Facebook, Google, Microsoft) in relation to your IdM/SSO solution?
- What are your biggest challenges for IdM?
- What is your biggest wish for IdM?
- In what way do you collaborate with other organisations (within the context of IdM)?
- Who are your users?
  - Do they all equally benefit from your IdM/SSO solution?
  - Are there users who do NOT benefit (as much) as others? Why?
- Do you have or think about a roadmap for IdM/SSO for the next 5-10 years? If yes, please share; if no, do you have any ideas about that?(your questions here…)

Federation-Related Questions for Campus IdP Operators:
- Have you heard of [insert national federation here]?
- Are you a member of [insert national federation here]?
- Do you operate an Identity Provider (IdP) and/or Service Providers (SP) for your campus?
  - What software do you run for your IdP? (e.g. Shibboleth, SimpleSAMLphp, ADFS, other)
- Why do you use [insert national federation here]? Which use cases does it support/solve for you?
  - What does it *not* solve?

Commented [17]: These questions seem to be too focused on single sign on - perhaps we would get different insights if we focus more connecting people to resources.

* Do you feel that connecting individuals to resources is a responsibility of your organization? why or why not? In what ways do you facilitate these connections?

* What challenges do you find in connecting individuals to resources?

* What social | regulatory | partnership | etc pressures do you receive that influence the choices you make related to these connections?

Commented [18]: These terms are SAML-specific, correct? Should we also ask whether they run OPs and/or RPs? AAs?

Commented [19]: I suppose SP/IdP are good enough; almost no one uses OIDC or has an AA currently within R&E AFAIK

Commented [20]: We may want to develop some protocol-neutral language for this before it goes public.

Commented [21]: We may not want to get this specific - what do you think?

Commented [22]: Shibboleth is de facto standard and potentially more amenable to enhancements as "our" identity tool. So I'd to learn from participants, "If you aren't using Shibboleth, why not? What are we missing in Shibboleth?"

- - What *should* it solve according to you?
- What works well about federations and what doesn't?
- For whom should federations be? (E.g. researchers, students, libraries, anyone in academia, …)
  - Which of those users do *you* serve mostly? (Not sure if this question is clear but I see that for our federation, most logins and services are enterprisy, not research oriented services)
- Do you trust that service providers are good stewards of the identity information you send them? If not, what do you need to trust the authenticity of service providers and that they are good stewards of identity information?
- If you DO NOT use federate credentials for your institution's users, why not?
  - No requests for access to federated resources?
  - Access accomplished by other means?
  - Lack of technical resources?
  - Other?

Federation-Related Questions for SP Operators:
- Have you heard of [insert national federation here]?
- Are you a member of [insert national federation here]?
- Does your application/service operate a SAML Service Provider?
- Is your Service Provider "collaboration ready" (can consume federation metadata files)?
- What software do you run for your IdP? (e.g. Shibboleth, SimpleSAMLphp, ADFS, other)
- Which of the following do you support:
  - IdP-initiated SSO
  - SP-initiated SSO
- Why do you use [insert national federation here]? Which use cases does it support/solve for you?
  - What does it *not* solve?
  - What *should* it solve according to you?
- What works well about federations and what doesn't?
- Which user communities (e.g. researchers, students, libraries, anyone in academia, …) do *you* serve mostly?
- Do you trust the identity information you receive from identity providers? If not, what do you need to trust the authenticity of identity providers and the information they provide?
- (your questions here…)

Commented [23]: We may not want to get this specific - what do you think?

Commented [24]: Shibboleth is de facto standard and potentially more amenable to enhancements as "our" identity tool. So I'd to learn from participants, "If you aren't using Shibboleth, why not? What are we missing in Shibboleth?"

- Do you have a well defined use case for federation
- Do you have a governance model already in place
- Do you have existing partnerships
  - Do you have mutual agreements in place for data sharing
    - What are the technical requirements for sharing
  - Have you identified your internal stakeholders
  - have you collected requirements and concerns from all stakeholders
- Do you have existing identity systems in place
  - how are these systems managed
  - do they inter-operate
  - how are trust boundaries set and managed
  - how is data stewardship determined
- Do you have in-house technical experts
- Do you have the human resources to manage
  - technical infrastructure
  - governance and management
  - negotiating and maintaining external partnerships/contracts

Thoughts about Risk in Identity Federations

There are four actors in federated identity: identity providers, service providers, end users, and federation operators. Each has its own risks, but our concern here are risks associated with actions taken (or not taken) by the other actors:

- Risks to IdPs
  - Bad custodianship of identity information by SPs
    - Improper release
    - Improper use

> **Commented [25]:** Thinking through how these risks could help inform our interview questions; I like how they could land in Judith's mention of the seven-question approach, specifically those example questions: "In the worst possible world what are your greatest fears?" or "What major constraints do you experience inside/outside the organisation/system?"

- - Spoofed RPs causing improper release
    - Bad metadata from FedOp
    - Key management failure
    - Protocol / software failure
  - Misbehaving users (sharing authentication tokens/secrets, ...)
  - Change to membership/subscription costs
  - Operational overheads/costs/knowledge
- Risks to SPs
  - Receipt of bad identity information from IdPs, especially, lack of receipt of important identity information
  - Unauthorized use of an authorized identity (compromised account - spoofed user)
  - Inability of IdPOs to react to federated security incidents
  - Inability of IdPs to support strong authentication
  - Spoofed IdPs resulting in bad identity information
    - Bad metadata from FedOp
    - Key management failure
    - Protocol / software failure
  - Inconsistent practices among IdPs
  - Lack of perceived shared ownership of the above risks
  - Change of federation model/costs
  - Operational overheads/costs/knowledge
- Risks to user
  - Improper release of information by IdPs and SPs
  - Improper use of information by IdPs and SPs
  - Access issues when ID changes due to change of institution
  - User experience poses a hurdle to getting things done, especially,
    - an entitled user can't login to a specific SP from a specific IdP due to insufficient IdP, SP, or federation practices
    - Insufficient clues provided on how to address a login malfunction
- Risks to federation operators
  - Receipt of bad metadata from IdPs and SPs.
  - Lack of relevance due to

Commented [26]: Should we focus this section on non-commercial, ie, academic SPs in this section, given that commercial SPs address their risks in contracts with each of their enterprise customers?

Commented [27]: Well, of course, the federations' participation agreements are also contractual mitigations, but in this list I tried to identify risks (that probably do not change over time) to help us focus on how mitigations will change in the future.

- - lack of assistance to other parties above in helping them address their risks
    - service, engagement, and training offerings not aligned with their memberships' needs
  - Reduced perception of value due to lack of focus on mission
  - Funding

Trusted Relationships for Access Management: The InCommon Model discusses the trust relationships that are needed to mitigate these risks.

Interview questions based on the "Seven Questions"

Guidance for the seven questions.
- If you could pose three questions to a clairvoyant who can foretell the future, what would you ask?
- In the best possible world what would you hope for?
- In the worst possible world what are your greatest fears?
- What pivotal events from the past few years provide good lessons for the future?
- What major decisions with long-term implications are faced at the moment?
- What major constraints do you experience inside/outside the organisation/system?
- If all constraints were removed, and you could direct what is done, what would you do?

Example

Commented [28]: Given it will be so hard to land on the 'ideal' set of questions right off the bat, we should probably settle on how we can manage our survey outreach iteratively, where we're able to 'experiment' in some sense, refine, circulate to a wider audience, repeat. Keeping in mind or larger timeframe of this work.

THE SEVEN INTERVIEW QUESTIONS

1. Clairvoyant	If you could speak with an acquisition oracle from 2025, what three things would you like to know about DAU?
2. Good Scenario	If DAU were thriving, growing and moving in a genuinely positive direction by 2025, what would be true of it?
3. Bad Scenario	If DAU were to collapse by 2025, what might have caused that collapse and why?
4. Inheritances from the Past	What surprised you about DAU in recent years? What have been the memorable "turns" and why?
5. Important Decisions Ahead and Priorities	What are the major challenges to be face by DAU and DoD acquisition professionals in the next five years? What are the obstacles to be overcome that keep you awake at night?
6. Constraints in the System and Changes that need to be made	What would hinder DAU and DoD acquisition from moving past these obstacles? What forces could constrain us?
7. Epitaph	Imagine that DAU is in danger of being completely cut. What is your argument for keeping it?

◯ Questions for external stakeholders

Possible questions for this group
- CLAIRVOYANT:

Formatted: Outline numbered + Level: 1 + Numbering Style: Bullet + Aligned at: 0.25" + Indent at: 0.5"