REFEDS ORCID WORKING GROUP REPORT

Authors: This paper represents the contributions of the full Refeds ORCID Working Group. (see the appendix) Significant contributions provided by the following individuals:

Melroy Almeida, Pål Axelsson, Tom Demeranville, Laure Haak, Keith Hazelton, Mark B Jones, Mikael Linden, Miroslav Milinovic, Laura Paglione, Chris Phillips, Hannah Short, David Walker[1]

Paper Type: Technical paper

1 Abstract

In early 2016, Refeds formed the ORCID working group to discuss several topics related to ORCID identifiers (iDs) and their relationship to the Federated Identity Management (FIM) community. This document outlines the discussions of this group through early 2017, and summarizes the opinions of the working group of how ORCID interacts with the FIM community and the rationale behind it. It covers three broad topics:

1. **ORCID as a Service Provider (SP).** ORCID became a SP in May 2016. This section discusses the SP use to date, and explores ways to increase the SP utility. (Section 2)
2. **ORCID as an Identity Provider (IdP)**. In some situations, ORCID is used as an IdP. This section explores this use including its limitations, opportunities, and future possibilities. (Section 3)

The members of the working group and significant contributors to this document are listed at the end of this document. (Appendix)

1.1 About ORCID

ORCID is a not for profit organization that has a stated vision of "a world where all who participate in research, scholarship and innovation are uniquely identified and connected to their contributions and affiliations across disciplines, borders, and time."[2] ORCID provides a registry of persistent, unique identifiers (ORCID iDs) for individuals to use with their name as they engage in research, scholarship and innovation activities throughout their careers. It also provides open tools that enable connections between identifier and information in workflows and systems worldwide. Established in 2012, ORCID has issued over 3.2 million

[1] Almeida: orcid.org/0000-0003-3522-7849, Axelsson: orcid.org/0000-0001-6217-5197, Demeranville: orcid.org/0000-0003-0902-4386, Haak: orcid.org/0000-0001-5109-3700, Hazelton: orcid.org/0000-0002-3174-899X, Jones: orcid.org/0000-0002-0666-9245, Linden: orcid.org/0000-0002-3634-3756, Milinovic: orcid.org/0000-0002-9603-3944, Paglione: orcid.org/0000-0003-3188-6273, Phillips: orcid.org/0000-0001-5567-4916, Short: orcid.org/0000-0003-2187-0980, Walker: orcid.org/0000-0003-2540-0644

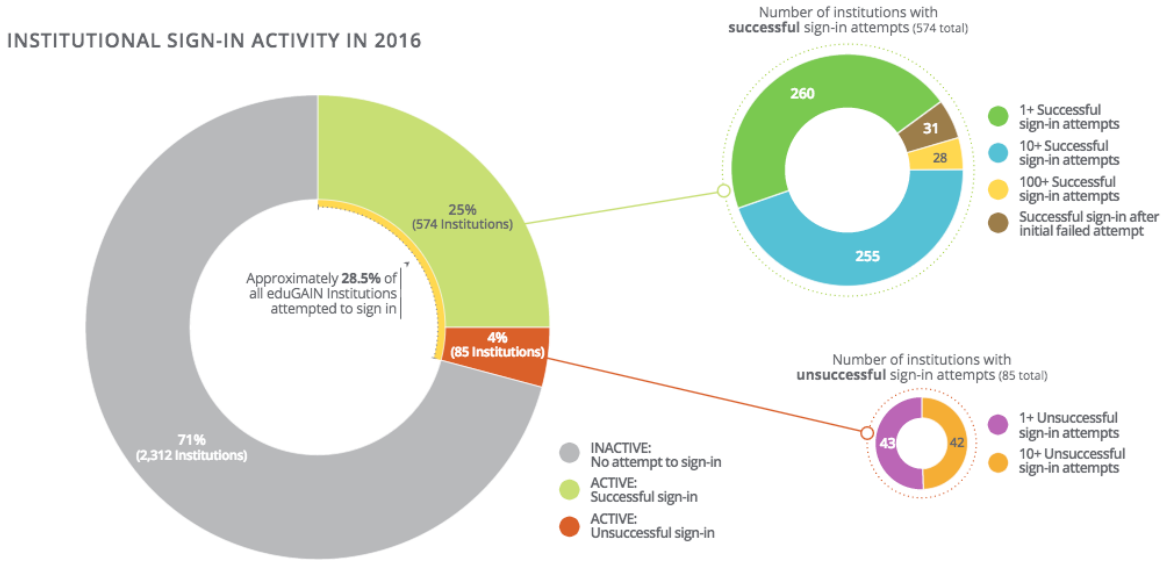
[2] ORCID website: https://orcid.org/about/what-is-orcid/mission

iDs, and over 650 member organizations globally support its mission financially and by adopting iDs in their workflows and systems.[3]

2 ORCID as an SP

2.1 What exists today

ORCID became a Service Provider (SP) registered in the eduGAIN interfederation service[4] in May 2016. It is categorized as a Research and Scholarship entity[5] by Refeds. The only Identity Provider (IdP)-dependent service that ORCID provides is institutional Single Sign On (SSO) for the user. Institutions listed by the discovery service are available as a sign-in option for ORCID users. As of January 2017, there have been attempted sign-ins from individuals from approximately 28.5% of all eduGAIN-listed institutions, with successful sign ins from 13,847 individuals across 574 institutions.[6]



ORCID outlines the specifics of their SP configuration on their website.[7]

Federation(s):	SURFconext eduGAIN interfederation service
Entity type:	Service provider
Entity ID:	https://orcid.org/saml2/sp/1
ORCID metadata:	Available in the Metadata Explorer Tool (MET)
Supported protocols:	SAML 2.0

[3] Meadows, Alice; Brown, Josh; Haak, Laurel; Paglione, Laura; Peters, Robert; Wright, Douglas (2017):ORCID Annual Report 2016.pdf. Figshare. https://doi.org/10.6084/m9.figshare.4810213.v1 Retrieved: Apr 05, 2017

[4] About eduGAIN http://services.geant.net/edugain

[5] Research and Scholarship Entity Category https://refeds.org/category/research-and-scholarship

[6] Meadows, A, et al. (2017): ORCID Annual Report 2016.pdf. Figshare. https://doi.org/10.6084/m9.figshare.4810213.v1 Retrieved: 21 29, Apr 05, 2017 (GMT) (Page 14)

[7] Sign into ORCID with Insittutional Credentials http://members.orcid.org/api/integrate/institution-sign-in

2.1.1 Consuming attributes

Currently ORCID requests and uses a limited number of attributes provided by IdPs. It requires at least one specific account-linking attribute to link an IdP account with an ORCID account.

2.1.1.1 Required attributes

ORCID requires a locally unique, persistent, non-reassignable identifier to link an institution account to an ORCID account. Specifically, any of the following identifiers will be accepted for this purpose[8] (presented in order of consideration by ORCID):

1. a persistent NameID (transient NameIDs will not be accepted)
2. eduPersonUniqueID (ePUID)
3. eduPersonTargetedID (ePTID)

Regarding eduPersonPrincipalName (ePPN): ORCID does not accept ePPN for the linking attribute, even for research and scholarship entities. The SP's stated reason is the career-long existence of ORCID iDs/accounts for individuals[9], as well as the chance, albeit small, of reassignment of eduPersonPrincipalName (ePPN).

2.1.1.2 Optional attributes

According to its documentation, ORCID will use the following attributes if provided by the institution, although none are required for the SSO service to work.

1. NAME (displayName, givenName, sn): If a name is provided by the institution, ORCID will use it in the following ways:
    a. Personalize the greeting to the user when they have signed in and are about to link the institutional and ORCID accounts.
    b. FUTURE: Enable addition of name to the individual's ORCID record as an "also known as" name(s) added by that individual (i.e., the individual is listed as the source).
2. EMAIL (mail): If an email address is provided, ORCID will use it in the following way:
    a. FUTURE: Enable addition of email address to the ORCID record.

Note: The addition and visibility of items on ORCID records is determined by the individual[10] (data subject) on the ORCID site. The individual may decline the addition of information, and may delete or change the visibility of added items at any time.

2.1.2 How accounts are linked

An Identity Provider (IdP) account is linked to the ORCID Service Provider (SP) account by having the user sign into each account, thereby making the link explicit. The IdP identifier (persistent nameID, ePUID or ePTID), is stored with the ORCID account. The next time that

---

[8] Sign into ORCID with Insittutional Credentials http://members.orcid.org/api/integrate/institution-sign-in
[9] ORCID's Vision, Mission & Values https://orcid.org/about/what-is-orcid
[10] ORCID Visibility Settings https://support.orcid.org/knowledgebase/articles/124518

the individual signs in with IdP credentials the IdP identifier attribute provided will match one that is already stored, enabling access to this ORCID account.

2.1.2.1 When accounts can't be linked

Given the number of identity providers that participate in the eduGAIN interfederation service, ORCID is unable to test each IdP to ensure that the required linking attributes will be provided.

When an individual is unable to link their IdP account, it is usually because one of the linking identifiers is not provided as an attribute. (See section 2.1.1 above.) When this happens, ORCID provides an information support screen that displays an error message and invites the user to send an email to the IdP support contact listed in the IdP metadata. This email includes suggested text directing the recipient to ORCID's documentation page. The email is also automatically copies the ORCID team.

Individuals are still able to use the ORCID Registry even if their accounts cannot be linked, however, they will need to do so using their ORCID sign-in credentials or a different linked account, such as a social sign-in.

2.1.2.2 Linking multiple accounts

Individuals may link multiple institutional accounts to their ORCID accounts. Once linked, they may use any of these accounts to gain access to the ORCID system. Individuals also can unlink any account at any time. ORCID provides additional information about linking and unlinking accounts in its user Knowledge Base[11].

2.1.3 Addressing incorrect account linking

In November 2016, ORCID received reports from end users that they were gaining access to incorrect ORCID accounts when they used their institutional credentials to sign in[12]. Upon further research, ORCID discovered that two different Identity Providers (IdPs) were sending the same linking identifier for all users at their respective institutions. ORCID temporarily disabled the service while investigating root causes, addressing the specific issues through established incident response channels, and implementing additional logs and controls to better identify similar issues in the future. Through analysis it was determined that the underlying cause for each of these issues was improper configuration of the identifier used for linking.

2.1.3.1 Discovering unauthorized access due to attribute issues

As the organization sending authoritative data, the IdP is responsible for ensuring the correctness of the linking identifier attribute. When there is a problem with this identifier, the IdP must address the issue. Unfortunately, the nature of federation means that incorrect data may be detected by a Service Provider (or worse, an end user) before being discovered by the IdP. Enforcement of correct data, therefore, must rely on a federated response to address

---

[11] Different ways to sign into ORCID https://support.orcid.org/knowledgebase/articles/892920

[12] The Duplicate-Identifier-Attribute-Issue And What to Learn From It https://blog.geant.org/2017/01/23/handling-security-incidents-in-edugain/

incidents of "incorrect data" that potentially involve both the receiver (SP) and sender (IdP) of the data.

As a result of the November incident, ORCID implemented additional controls to better detect potential incorrect data and protect users against unauthorized access due to incorrect linking identifiers. Specifically, ORCID implemented the following:

1. **Storage of ePPN and other identifiers.** Although ORCID still does not use the ePPN for the linking of accounts, they now store and check the ePPN prior to providing access to an ORCID account. If the ePPN does not match that of the original connection, the user is requested to re-link the accounts. Similar checks are in place for any other identifiers that are provided as attributes.
2. **Additional logging.** ORCID has implemented additional logging to help troubleshoot other issues if they come up.

2.2 Increasing SP utility

While nearly 14,000 IdP users for a single SP is high by many standards, the number only represents a tiny fraction of the over 3.1 million users of the ORCID registry. The working group reviewed these connections and considered how to increase use by individuals and utility to institutions as a result of the connection.

2.2.1 Increasing use of IdP-ORCID account linking

Any increased utility to institutions is dependent on regular use by individuals of the institutional sign-in for ORCID. The working group agreed that improvements can be made in workflows leading to institutional sign in on the ORCID site.

2.2.1.1 Suggestions for ORCID

1. **Enable link to an institutional account when already signed into ORCID.** Currently accounts can only be linked during the sign-in process. Allow the user, via the settings page, to initiate an IdP login at their home institution and link it with their ORCID account.
2. **Enable link to an IdP account during the registration process for a new ORCID.** Currently IdP accounts can only be used to log in after the account has been created. Federated login should also be made available at the time of account creation.
3. **Support URLs to enable sign in without the Discovery Service[13].** Enable organizations to direct their constituents sign into the ORCID SP by going directly to their IdP sign in. This process would replace the need for individual users to find the IdP listing from the discovery service presented on the ORCID sign in page, thereby saving the user a step in the sign in process, and will further encourage account linking. *Note: General WAYF-less service using discovery algorithms, for example from email addresses, is not recommended at this time.*

[13] Also known as WAYF (Where Are You From): https://wiki.edugain.org/Federation

2.2.1.2 Suggestions for IdPs

1. **Socialize the benefits and use of ORCID iDs.**
   Organizational promotion of the service is important particularly because, to individuals, the use of the service is generally invisible when working well; the individual signs in the first time, and can forget about it thereafter (but, see 2.2.2).
2. **Provide resources to help individuals sign into ORCID with institution credentials.**
   Institutions should provide help pages, library resources or links to ORCID resources to assist their users in signing into ORCID with institution credentials. ORCID provides some "starter resources" at members.orcid.org.
3. **Increase utility to individuals by asserting affiliations to ORCID records.**
   IdP home institutions should consider using ORCID's API to provide affiliation assertions on ORCID records so that they may be consumed by others viewing the individual's ORCID record. Note that this model of providing affiliation information is different from attribute-derived assertions (described further in section 2.2.5) By providing this user benefit, home institutions will help increase the utility of the affiliation link and hopefully support adoption of ORCID iDs. There are two main benefits that can be realised through this model for adding the affiliation information:
   a. First, the institution could update the record to contain affiliation (education and employment) entries with strong provenance as they are the affiliated institution. The information provided can match otherwise publicised information about the individual, for example, information from library services.
   b. Second, ingest of the ORCID iD into home institution systems can be used to provide internal benefits such as simplified/streamlined workflows in other parts of the research lifecycle.

2.2.2 Improving account handling when IdP access is discontinued

One side-effect of encouraging federated (or social) login is that the original account details are often forgotten by the end user. The group noted that the ORCID iD provides a persistent (career-long) identity component of the login interaction, and must be designed to outlive the IdP sign-in association. ORCID should take steps to ensure that the account can be recovered if, for example, the email account or institutional account of the user becomes unavailable. The group anticipated that without a process for managing this, it would likely result in multiple record creation when the users lose control of their accounts.

2.2.2.1 Suggestions for ORCID

1. **Encourage the inclusion of multiple email addresses.**
   ORCID should further promote and increase access to its existing functionality for users to include more than one email address associated with an ORCID account. This inclusion will help increase the likelihood that individuals will be able to regain access to their accounts in the event of an institution change.

2. **Establish other methods of account access.**
   Some examples may include mobile phone verification or other non-email dependent password reset option.
3. **Increase awareness of account deprecation process.**
   For when duplicate accounts are made, ORCID has a deprecation process that individuals may use to combine accounts, and have all ORCID iDs point to a single primary iD that is used by the individual. While this process exists, users may not know about or understand it. ORCID should promote its existence and benefits

2.2.2.2 Suggestions for IdPs

1. **Add ORCID to employee/student exit checklists.**
   For institutions that have communication checklists and communications for exiting employees and students, information about ORCID should be included to remind the individual that the ORCID account travels with him/her throughout his/her career. Communication may include information about how to de-link institution sign in, how to re-establish independent access, and/or how to include an additional email address to one's account to ensure that access is maintained. For those who have established ORCID OAuth permissions, communications may include reasons why the individual may want to persist these permissions, for example, to help update affiliation information on the ORCID record, read records for post-exit reporting, maintain access to certain resources via an ORCID sign-in, etc. This also enables the institution to modify the affiliation of the ORCID record to include end dates of employment or education activities.

2.2.3 Proactively identifying identifier issues

In examining the root causes of the November 2016 incident described in section 2.1.3 above, the working group discussed ways in which similar challenges might be identified proactively in the future. Although the issue can be remedied through incident response, the potential harm to the individual may already have occurred through unauthorized access to his/her account. In the situations where unauthorized access due to misconfiguration was not discovered programmatically, there is a reliance on individuals to report the issue that they have gained access to someone else's account. The person whose account was accessed would have no knowledge of the breach until being informed by ORCID or their institution. Informing the affected users can have its challenges, as the affected user is not involved at the time that the issue occurs, and the trust dynamic at the time of the incident tends to be between the user and the SP, not the IdP where the issue had originated[14].

2.2.3.1 Suggestions for future exploration by the FIM community

1. **Explore methods for testing identifier attributes used for account linking.**
   To test for identifier attribute errors, usually at least two test accounts are needed to

[14] During the November incident, ORCID informed the users of the unauthorized access. Despite the problem being characterized as a misconfiguration at the user's institution, the individuals saw this as a problem caused by ORCID because it occurred on the ORCID site.

ensure that they are not issuing duplicate attribute values. To date no known widespread tests exist to make these discoveries. In the case of ORCID, it is problematic to wait until discovery of such an issue by the SP. This suggestion is to seek ways to work with the community to establish better pre-incident misconfiguration discovery to proactively discover and address challenges in the future. This exploration may include testing tools, a set of guidelines, or other methods.

2. **Increase awareness of identifier configuration methods.**
   In the cases where there were challenges, there was a combination of low use (of the vendor system or the attribute being sent to ORCID or both), and lack of SAML know-how that triggered an unintentional misconfiguration that led to inaccurate unique identifiers (i.e., the same IDs for all users) being sent as a linking identifier.
3. **Make specific recommendations on the R&S category for inclusion of non-reassignable identifiers, persistent NameID, ePUID, ePTID.**
   In the case of ORCID, some institutions specifically configured the required linking ID attributes only for the purpose of supplying them to this single SP. As a result, discovery of potential challenges can be slow, or not discovered at all because of lower use. Broader inclusion of these identifiers in the R&S category can lead to greater use of these identifiers.

2.2.4 Increasing ORCID's incident reporting capabilities

As a result of the November 2016 incident, ORCID also learned that point to point incident resolution works best when you have a relationship with the organization, a conclusion also drawn by the AARC work on Security Incident Response Procedures[15]. For SPs that enable sign in using institutional credentials, the SP doesn't necessarily have direct connections with each of the IdPs from which someone can sign in, particularly when broadened to the context of the eduGAIN interfederation. As a member of the federation, the SP and others all agree to operate in a similar way with similar rules. While this arrangement makes it quick and easy to enable sign in for individuals covered the nearly 3000 IdP that are part of eduGAIN, a direct relationship with the institutions involved can help speed resolutions when needed. Leveraging existing relationships in identity federations are also helpful, for example, relationships between IdPs, their Federation operators and eduGAIN. The working group makes the following suggestions:

2.2.4.1 Suggestions for ORCID

1. **Adopt and support of Sirtfi.**
   Sirtfi, Security Incident Response Trust Framework for Federated Identity, was developed in 2016 to ease collaboration in the event of a security incident impacting multiple organizations in a federated infrastructure. Adoption of this framework can help mitigate some of the challenges encountered by ORCID when direct relationships with IdPs were not established.

[15] https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf

2. **Increase understanding of established escalation procedures.**
   With the challenges in November being ORCID's first encounter with an incident, it was not well-versed in incident procedures, timelines, or communication norms. ORCID should collaborate with members of the community to improve and increase knowledge of documentation and guidelines for SPs who may discover incidents.

2.2.4.2 Suggestion for IdPs

1. **Adopt and support Sirtfi.**
   Sirtfi will be stronger if more in the community are adopting it. A goal should be for the extended identity management community to use this evolving standard to handle incident responses. It is expected that SPs like ORCID are likely to require Sirtfi in the future.
2. **Minimally include current security contact in IdP metadata.**
   All IdPs should explicitly lists a security contact in their metadata, even if this contact matches that of their technical contact. By listing this contact, the IdP also signals its commitment to security.

2.2.4.3 Suggestions for future exploration by the FIM community

1. **Consider the ORCID November incident as a use case.**
   Some aspects of the ORCID incident may expose unique considerations for future incident response procedures. How should the community handle communication to end users affected by incidents? What are end user expectations for response time? How broad should notification be to potentially affected members of the community? Should those unaffected be informed, and if so, to what extent? This use case can provide a lens for exploring some of these questions.

2.2.5 Creating affiliations and exposing federated login information

Federated login is difficult to get right. One of the many things that must be considered is the fine line between gathering information because it's useful to the user and gathering information because it's useful to the service. Many do this badly, but the group considers ORCID to be walking this line well. They consider ORCID to be well positioned as recorder of information, with the value of that information measured by perceptions of the strength of assertions.

One set of information that is strongly asserted but currently not exposed as part of the ORCID record is how and where people log into ORCID. There are several reasons for this:

- The relationship between a federated sign in and the institution is complex. While there is a defined eduPersonAffiliation vocabulary, its usage varies between countries and individual institutions.
- It is difficult or impossible to map eduPersonAffiliations to the existing education and employment affiliation types within ORCID.
- If 'federated affiliations' were propagated, there is a risk that they are considered a concrete affiliation in the ORCID sense of the word. The reality is that is simply

states someone logged in with an IdP at a particular institution, which could have, for example, guest accounts enabled. This risk can be extended to include perceptions of greater strength, when none is in fact present.
- There's the risk that an affiliation of this kind would be considered current, when that cannot be proven without reference to the original asserting identity provider.
- User concerns around privacy.

Other discussions highlighted that many institutions only hold information on current affiliations not historical ones.

2.2.5.1 Suggestions for ORCID

1. **Add & expose information of when and how someone last signed into ORCID.** The group considers "This person was active at this place at that time" useful information that should be exposed if possible. Use cases included scenarios such as evaluating past work and investigating credibility. The group stated that as a privacy driven service, ORCID is well placed to put the privacy settings of this type of affiliation information under direct user control, on an opt-in basis. Effective dating would be required, including the last login. This should not be considered a 'best by date', but rather something people can draw their own conclusions from.
2. **Explore other services that record and expose sign-in data.** To better understand potential issues with exposing the functionality described above, ORCID should explore other systems that expose similar data to better understand potential issues and the ways they may be dealt with.
3. **Consider adding affiliation information based on attribute release.** ORCID's model is for organizations to explicitly push related data into individuals' ORCID records. ORCID should consider enabling the addition of affiliation data based on the sign in at an institution based on the attributes released. Note that due to the nature of affiliation metadata, affiliations generated from attributes may not be as well defined as that received via the API.

3 3 ORCID as an IdP

3.1 What exists today

From its beginnings, it has been possible to use ORCID authentication using its OAuth-based permission protocol[16]. Although some organizations are using ORCID sign-in for authentication purposes, ORCID has downplayed this functionality because, unlike many identity provider services, ORCID does not attempt to perform any identity proofing of the users of the registry.

The working group explored this topic with the objective to provide greater context around the limitations of the use of ORCID as an IdP, and to provide guidelines on ways that ORCID may be effectively used for this purpose.

[16] An example of a journal submission system is enabling sign in via ORCID credentials: https://vimeo.com/206612019?ref=tw-share

3.1.1 ORCID user authentication use cases

There are several reasons why a site or project would consider the inclusion of ORCID as a method for sign in. In some cases access to a system may need to persist beyond the expected relationship that the individual has with their institution-based sign in. Examples include a graduating student that is included on a project requiring system access, or to provide career-long access to a resource such as a paper that the individual authored. Alternatively, a system may opt to increase sign in options for individuals when authentication is important, though identity proofing and/or authorization information from the IdP is not a priority.

3.1.2 The ORCID OAuth workflow

ORCID supports the commonly seen 'three legged' OAuth workflow, whereby a user grants a third-party service permissions to interact with their record. These workflows are usually initiated by the third party, but in a limited number of cases (referred to as 'search and link wizards') ORCID will initiate the workflow from within the registry site. These are restricted to general purpose tools such as Crossref and Datacite metadata search.

3.2 Increasing IdP utility

3.2.1 Two factor authentication

The group does not considers two-factor authentication to be a necessity for connection purposes, but recognizes that it may be critically important from an end-user's point of view. Multi factor authentication can be used to increase confidence that the service is interacting with the same user who logged in previously, though it doesn't increase confidence in proving (or disproving) the identity of who the user is in the first place. Concerns were raised over the confusion this may cause to implementers.

3.2.1.1 Suggestions for ORCID

1. **Add two-factor authentication to ORCID sign in.**
   What multi factor authentication could do is provide greater security for the ORCID individual user. This security and confidence would start when the second factor was registered, either directly with the ORCID system, or by linking a federated identity that uses multi factor authentication.
2. **Provide clear guidelines and interpretation aids on implications.**
   Clearly describe that two-factor authentication provides stronger authentication confidence, not stronger identity proofing confidence.

3.2.2 ORCID and strong self-service identity vetting

Identities within ORCID are self asserted. This is in contrast to the majority of FIM based identity solutions, the exception being IdPs like UnitedID. The group considers self-asserted identity to be a unique property of ORCID and differentiator rather than an issue to address - *"the beauty is that ORCID doesn't validate identity."*

Connections to publishers and institutions by researchers constitute a form of low-level identity proofing. As researchers couple their ORCID ID to their scholarly activities, for example, linking a publication during the manuscript submission process, their identity gradually becomes very reliable. If an institution or publisher is listed as the source of information it is assumed that that source performed some kind of identity check itself.

It is unclear if publishers or institutions are more useful for identity proofing purposes, although the group does note that while institution identity vetting varies from place to place, publisher vetting is universal. In any case, the group considers 'validated' affiliation assertions from institutions useful.

3.2.2.1 Suggestions for the working group

1. **Develop guidelines for interpreting self-service identity proofing**
   Traditionally, strong authentication is a combination of strong identity vetting (face-to-face at a registration desk) and two factor authentication. Of those two, strong identity vetting is the tricky and expensive part. The group should work to understand how the concept of strong self-service identity vetting could work without a face to face component. The group should focus on how the connections ORCID has with institutions, publishers and researchers could be leveraged to make strong self service identity vetting work in practice.
2. **Consider implications for access right binding to an ORCID iD**
   A researcher's ORCID record represents their scientific persona/career/merit and that is often what the Data Access Committee wants to assess when the researcher applies for access rights to a sensitive dataset. Sometimes it can be even more important than knowing that their institution has performed strong face to face identity vetting. The group should explore if and when it would be appropriate to bind a researchers' access rights to services to their ORCID ID and use the ORCID API for their authentication

3.2.2.2 Suggestions for ORCID

1. **Consider differentiating between different types of associations.**
   It would be useful if there was a way to distinguish between the associations made during the submission process and those made in other ways, as the identity proofing involved differs. Work is needed to understand the various types of associations.

3.2.3 ORCID as an attribute store

The attribute store concept is intended to enable service providers to retrieve information from the ORCID registry based on federated login information. Specifically, a federated unique identifier coupled with the entity ID of the IdP would be resolvable to an ORCID ID. This functionality would depend on the concept of the registry exposing a user's federated login information, as discussed in the SP section of this document.

The most useful attribute the ORCID registry can provide is the ORCID identifier itself, possibly provided alongside a display name. Other information attached to an ORCID record

should remain the responsibility of the ORCID API and can be retrieved using the ORCID identifier as provided by the attribute store. Much of the value of using ORCID in this way is that the individual is in control of which attributes are released via the ORCID privacy controls.

As ORCID works within eduGAIN, it is envisaged that this functionality could be available to all members of eduGAIN. However, the group noted that it is important to be able to identify and prevent misuse so measures would need to be in place to revoke access to the attribute store. What counts as misuse will need to be considered on a case to case basis.

3.2.3.1 Suggestions for the working group

1. **Develop a "broad-stroke specification" for ORCID as an attribute store**
   Based on models already in use, and the expected utility to the community, develop a high-level, use-case-style specification for ORCID as an attribute store for ORCID consideration for future development. Consider the role of R&S attributes in this implementation.

3.2.3.2 Suggestions for ORCID

1. **Explore options for ORCID as an attribute store**
   ORCID currently supports OAuth as the primary means of authentication and authorisation. This, possibly combined with a custom API call for resolving federated identifiers for ORCID identifiers or the existing search API is sufficient for the use case outlined above.

4 Conclusions

As outlined in this report, there are several recommendations for ORCID, IdPs, the FIM community and the Refeds ORCID Working group. The next task for the working group is to facilitate the adoption of these suggestions. This work will continue via the Refeds working group over the remainder of 2017. In addition to these suggestions, the working group also recommends that ORCID continue to take a leadership role in

1. Implementing best practices established by the community
2. Work with other SPs to advocate for SP needs and illuminate SP unique challenges
3. Share ORCID's operational approaches as an SP for comment and feedback from the community, as well as potential guidelines for other SPs where appropriate

The Refeds ORCID working group has made significant progress in unpicking the complex interactions between ORCID and federated identity. It is, however, an ongoing process and it is recommended that the working group continues to meet and discuss the recommendations within this document as well as future developments. New members are of course welcome to join the group and discuss this document with the people that created it as well as contribute to future recommendations and solutions.[17]

[17] ORCID Refeds Working Group Page: https://wiki.refeds.org/display/GROUPS/ORCID

APPENDIX: Working group members & contributors

Ashley Rustin
Bob Cowles
Scott Cantor
Chris Phillips
David Bantz
David Walker
Eskil Swahn
Hannah Short
Heather Flanagan
Jim Basney
Johan Bergstrom
Keith Hazelton
Ken Klingenstein
Laure Haak
Laura Paglione
Leif Johhanson
Licia Florio
Maarten Kremers
Mark Jones
Melroy Almeida
Mikael Linden
Miroslav Milinovic
Niels van Dijk
Nicholas Roy
Pål Axelsson
Pete Birkinshaw
Peter Gietz
Rhys Smith
Scott Koranda
Steven Carmody
Tom Demeranville
Terry Smith
Warren Anderson