For Discussion: ORCID as IdP

Even before ORCID launched, there have been questions, comments and suggestions about ORCID's role in representing the identity of a person, and whether ORCID should take on this role in addition to that as an providing an identifier registration service. The context of this conversation is most often in the context of Identity Access Management (IAM).

There are compelling cases for and against ORCID as an identity provider, and wise advice for ORCID to have a well thought-out position.

The purpose of this discussion stub is to outline and explore this topic in its full complexity. For clarity, let's use Nathan Dors' Oct 28, 2014 presentation Intrduction to Identity Management as a baseline of what we're talking about for IAM. The resulting information also will serve as one of the points of input for ORCID's final position and policy.

NOTE: In trying to frame the discussion, a critically important topic may have been completely left out. Please add other areas if you feel they are important for this discussion.

Related Resources

- InCommon IdP of Last Resort WG List of Requirements
- Internet2 IdPoLR Working Group Final Report
- REFEDS IoLR Working Group
- AARC Sustainability Models for Guest IdPs

Should ORCID be considered an IdP?

The arguments for ORCID being an IdP, also suggest that there be clarity in the limitations that ORCID has in this role. For example, ORCID should be clear about

- what it can assert with confidence
- the level of confidence in other associations between items and the ORCID, for example, information on an ORCID record.
- the level of assurance about the identity of the individual signing in
- when using ORCID as an IdP may be useful
- how ORCID handles notification of credential/access incidents

Arguments against ORCID being an IdP usually state similar areas where clarity is needed, and also argue that serving as an Identity Provider is not core to ORCID's stated mission which is:

VISION: ORCID’s vision is a world where all who participate in research, scholarship, and innovation are uniquely identified and connected to their contributions across disciplines, borders, and time.

MISSION: ORCID provides an identifier for individuals to use with their name as they engage in research, scholarship, and innovation activities. We provide open tools that enable transparent and trustworthy connections between researchers, their contributions, and affiliations. We provide this service to help people find information and to simplify reporting and analysis.

What else should be considered? How do these points stack up to your use cases?

Use cases

<to be included - use cases that help illustrate situations where ORCID should / should not be considered as an IdP.>

1. ORCID should be an Identity Provider of Last Resort according to ORCID's mission to "provide an identifier for individuals to use with their name as they engage in research, scholarship, and innovation activities." No identity proofing needed beyond email address validation. See InCommon IdPoLR WG Final Report for more detailed requirements and non-requirements. (James Alan Basney)
2. ORCID should be able to release eduPersonOrcid to an university to provide a mecanism for identity linking. This is a way a local user at the university can prove possession of a ORCID and do a verified linking of his ORCID to his records at the university. (Pål Axelsson)

What is an identity provider? Where does ORCID stand?

What are some of the traits of identity providers. (It doesn't have to be of all identity providers.) How does ORCID compare on these traits? Should ORCID do anything differently? Why or why not?
<table>
<thead>
<tr>
<th>#</th>
<th>What do identity Providers do/ provide? (even if only sometimes)</th>
<th>How does ORCID currently stack up in this area?</th>
<th>What is the gap (real or perceived) that ORCID has in fulfilling this area?</th>
<th>Should ORCID be doing anything in this area? If so, what?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identity proofing this person is who (s)he says (s)he is</td>
<td>The more publications the person has coupled to their ORCID ID (in the manuscript submission phase) the more reliable the identity proofing is. (Mikael Linden) - Incentive alignment of correct association. The ORCID SP does identity linking between home organization and ORCID. This type of linking is proofing information. (Pål Axelsson) - In-person establishment of identity checking.</td>
<td>For IdP0LR, current ORCID email verification processes are sufficient and self-asserted displayName is fine. (James Alan Basney)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Provide a unique identifier so you know this person is the same person that signed in last time.</td>
<td>This is ORCID’s mission. (James Alan Basney)</td>
<td>ePPN, ePTID and EPUID are the widely used identifiers, as an IDP ORCID should populate them? (Mikael Linden)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Provide attributes to assist others to understand who the person is for the purposes of access and privileges</td>
<td>ORCID requires explicit consent from the user to release any attributes (including name) other than the ORCID ID.</td>
<td>Provide minimal R&amp;S attributes (mail, displayName) for interoperability/usability, not for access/privileges. (James Alan Basney) Provide eduPersonOrcid for identity linking at university level. (Pål Axelsson)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Establish inclusion within a “community” the presence of a person from an identity provider signals that person’s inclusion in this community.</td>
<td>No. (James Alan Basney)</td>
<td>When registering an ORCID ID, ORCID could let people download a smartphone app (TIQR or similar) for 2FA. (Mikael Linden)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2 factor authentication</td>
<td>ORCID Supports only password authentication. (Mikael Linden)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>