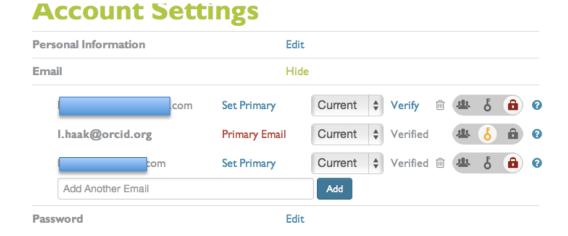# ORCID Functionality and Plans

Duplicate Detection, Merging and Deprecation, and Errors
For each new identifier registration, ORCID checks against the Registry for matching name/email address, and when a possible match is found, presents that to the registrant to claim. Earlier this year, we instituted the ability to link multiple email addresses with an ORCID record to support this duplicate detection process (http://orcid.org/blog/2013/06/20/new-features). Users may add current and past email addresses using their account tools, or record creators are able to populate a record with multiple email addresses upon record creation using the Member API. The user has the ability to set one email as primary, for receiving notices from ORCID, and can set privacy on each address separately (see image below).

In the event that a user has more than one ORCID iD, there are two options: maintain these two records, or (with user permission) merge the records and deprecate one identifier. The deprecated iD is not deleted, but rather associated with the primary iD. Searches for the deprecated iD resolve to the primary iD.

While ORCID does not control the data in the ORCID Registry or individual records, it is committed to supporting a transparent and accurate data environment. To that end, ORCID maintains a log of when and by whom data in the Registry are added, edited, or deleted. In the event that a record is created falsely or a false claim to information is contained in an ORCID record, ORCID has a Dispute Resolution Procedure (http://orcid.org/orcid-dispute-procedures) to verify and correct data that a user is not able to correct on their own.

Issuing of IDs
ORCID iDs are issued using a random number generator, and incorporate a checksum, so it is unlikely that consecutive persons by alphabetical order or order of record creation through batch upload using the member API would have a consecutive ORCID identifier number.

Affiliations
ORCID will be rolling out its Affiliations module in Autumn 2013. We did not include this functionality in the initial release as we felt it was imperative to link to an organizational identifier, rather than allow the user to enter affiliation as a free-text field. As recommended by NISO, we will be using ISNI organizational identifiers, and obtaining these and organizational

metadata through Ringgold, an ISNI registration agency. In addition, we are developing a specification that is flexible enough to support other inputs for organizational iDs should that need arise. We will be requesting that ORCID members provide us their ISNI/Ringgold organization identifier upon use of the Member API, and for any member that is creating ORCID identifiers for their employees, they must include their Org_ID in the batch upload. As with adoption of ORCID, establishing a community of practice around management of organizational identifiers will require a concerted effort, but current indications suggest the community is willing to make this effort. We have been talking with a number of community members (ProQuest, Eagle-I, VIVO, and UK funders) who are interested in helping to curate the RingGold/ISNI organization database. The RingGold and ISNI databases do not yet support display of organization hierarchy, but they do maintain relationships between organizational components, so with the participation of the community it may become possible to provide more granularity in this respect.

Third-Party Claims
One of our major 2014 development objectives is supporting third party validation of claims in the ORCID Registry. This would include the ability for employing organizations to validate affiliation and works claims, and claims by other member organizations on links to works. We are currently developing high-level specifications for this functionality, and expect to complete this planning process by the end of 2013. Third-party claim on affiliation could be an important component allowing ORCID identifiers to be used in authorization/identity management systems. CrossRef and APA are two of several organizations examining ORCID in single-sign-on schemes, using this approach.

Current member list
As of the beginning of August, 2013, ORCID had 70 members from a broad cross-section of the research and scholarly community. Members are listed on the ORCID Webpage, and a list by sector is provided below.

Publishers	Aries, Copernicus, Elsevier, EDP Sciences, eLife, Epistemio, Hindawi, Infra-M Academic Publishing, Karger, Landes Bioscience, Nature, Peerage of Science, ScienceOpen, Springer, Wiley
Associations	AAAS, American Chemical Society, ACSESS, American Geophysical Union, American Psychological Association, American Physical Society, American Society of Microbiology, American Society of Civil Engineers, Association for Computing Machinery, Modern Language Association, OSA, Royal Society of Chemistry
Funders	US Department of Energy, US Food and Drug Administration, Japan Science and Technology Agency, US National Institutes of Health, UK National Institute of Health Research, Wellcome Trust
Universities and Research Organizations	Boston Univ, CalTech, Chalmers Univ Technology, Chinese Academy of Sciences Library, CERN, Cornell Univ, EMBL (EBI), FHCRC, Glasgow Univ, Harvard Univ, IFPRI, KACST, KISTI, MIT, MSKCC, National Institute of Informatics, NYU Langone Medical Center, Riga Technical Univ, Univ Oviedo, Univ Zaragoza, Univ College London, Univ Cambridge, Univ Hong Kong, Univ Kansas, Univ Manchester, Univ Michigan
IDs	ResearcherID, Scopus
Repositories and Profile Systems	Altmetric, ANDS, AVEDAS, British Library, Copyright Clearance Center, CrossRef, DataCite, F1000 Research, Faculty of 1000, figshare, Knode, OCLC, PubMed Europe (EBI), Symplectic, Thomson Reuters

Physical Location of Servers
ORCID data is hosted by Rackspace. The basic servers are all located in Texas. Our database backups are stored in Dallas and Chicago. Our Content Delivery Network (CDN), the primary purpose of which is to speed up page loads, is hosted in various locations around the world so that the data has shorter to travel to be delivered to the user's browser. The CDN stores data-intensive static files like images and video, but no personal information. A more geographically-distributed server model is desirable, but requires substantial initial and ongoing capital and resource investment. We will re-evaluate server distribution when the ORCID Registry is large enough to justify the additional complexity.

https:
ORCID queries are managed using https://. The Registry was launched without https:// support, but this was one of the first upgrades released in 2012.

Integration of ORCID iDentifiers in Grant Applications
In addition to being integrated into grant application systems at the US National Institutes of Health, US Department of Energy, the Australian National Health and Medical Research Council, and Wellcome Trust, ORCID identifiers have been recommended as a component of the Horizon 2020 grant application process.

Advocacy and Outreach
ORCID just launched its Ambassador program. A component of this program is production of one-pagers, slide decks, videos, posters, bookmarks, and other materials, which will be made available to program participants for sharing at meetings and presentations. For specific community needs and presentation, such as Data Privacy, ORCID and we will work with you to research the issue and produce appropriate documents.   We also welcome suggestions for community contacts and prospective integrations, such as the Repository Junction Broker. You may submit ideas or requests to our iDeas Forum, our support desk (support@orcid.org), our Director of Community (community@orcid.org), or directly to the Executive Director (l.haak@orcid.org).