APA VIVO: A Semantic Framework for Scholarly Identity and Trusted Attribute Exchange

Hal Warren and Eva Winer

American Psychological Association, Washington, DC, USA
{hwarren,ewiner}@apa.org

Abstract. In this paper, we describe a semantic approach to scholarly identity and scientific attribution based on a trust extension of VIVO, an open-source semantic social network platform for scientists. The Publish Trust pilot demonstrates how researchers can extend and manage verified claims of authorship in a semantic framework using VIVO instances and open identity technologies.

1 Introduction

This paper describes a pilot that examines the feasibility of adding trust values to online identities for authors of scholarly publications. Existing online networks for scientists (BiomedExperts, iamResearcher, etc.) do not include mechanisms for verifying self-asserted authorship claims. The pilot, developed by the American Psychological Association (APA), uses open source VIVO[1] semantic technology and the Open Identity Exchange (OIX) Trust Framework Provider[2] to deploy an author identity platform and track scientific attribution. VIVO is an ontology-driven Java application designed to facilitate the discovery of research expertise and enable scientific collaboration across disciplines. There are currently 50 VIVO instances at the leading research universities in the US, and about 20 international projects. VIVO is built on the Jena semantic web framework, and models researcher profiles based on core Vitro ontology, originally developed at Cornell University [1]. VIVO harvests data from verified sources like publication databases (PubMed, APA PsycNET), institutional human resources databases, grants, and data repositories, and ingests them into the matching researcher profiles. This data is represented as RDF and published as Linked Data.

2 APA VIVO Framework and Trusted Attribute Exchange

We developed the Publish Trust Framework (PTF) pilot to deploy and test reliable methods for trusted attribute exchange as an extension of VIVO semantic framework, where URIs identify people, groups, publications, events, equipment, etc. The APA pilot is centered on authors of articles published in APA's scholarly peer-reviewed journals, and produces publisher-validated trusted assertions of authorship, enabling scientists to reliably aggregate their works and connect with other experts in their field. We proof author accounts using APA intake forms at apa.publishtrust.org. Authors set conditions for trusted authorship attribute extension and retraction after the account holder identity is verified through a surface mail-back method.

[1] http://vivo.sourceforge.net/

[2] http://openidentityexchange.org/

Once the account is activated, authors are presented with a list of works they can claim. As attributes of authorship are extended from author.publishtrust.org to the APA VIVO profile, the status of the individual's VIVO page changes from "unverified" to "confirmed”. Data for a community of over 3,000 authors is now available on APA VIVO instance https://vivo.apa.org.

Two-factor trusted claims of authorship are managed via the US government-approved Open Identity Exchange (OIX) and Attribute Exchange Network (AXN), a secure closed network of Identity Providers, Attribute Providers, and Relying Parties that supports trust assertion payload delivery and consumption.

Exchanges result as authorized RDF-XML payloads that can be included within other VIVO instances as Relying Parties. This is indicated by a trustmark, which links back to RDF-based metadata supporting the claim. Attribute provider credentials contain a description of the assertion including a description of the source, the relationship between the source and the account holder, and a definition of the assertion made transparent at the base URL for the attribute. Authors remain in control of the privacy constraints for the attributes they have extended, and can retract those claims at their discretion. Claims can be challenged by other known identities in the framework, or anonymously.

The framework also provides an ability to anonymously assert expertise in a certain field. A clinical psychologist, for example, can offer advice on Facebook as a specialist on eating disorders. Anonymous ability is especially important in animal research and other sensitive research areas.

Publish Trust will allow researchers to validate many of the attributes that they assert on their profile. New APA-backed attributes, including trustmarked reviewer contributions, scientific Board and Task Force membership, and service to the profession will be harvested and added to the framework in the next phase of the pilot.

Cornell University is participating in the pilot as the first consumer of APA author attributes. Trust assertions move within a closed network at different levels of assurance. Using InCommon Federation SAML-based authentication as the single-sign-on mechanism allows attribute exchange and linking to APA attribute servers and resources from the account holder's Cornell VIVO profile. Each attribute provider and consumer server is authorized by InCommon protocols and SSL Certificates and meets National Institute of Standards and Technology Levels of Assurance-2 (NIST LOA-2) requirements [2].

For future work, we also aim to integrate PTF attributes via VIVO with ORCID (Open Researcher and Contributor ID) API and other author identity and disambiguation initiatives, engineer attribute binding using OpenID Connect protocol, and develop reputation and trust assessment algorithms for PTF assertions.

In conclusion, trusted attribute exchange creates a fundamental new opportunity for the advancement of science by improving scientific contributions through increased velocity in scholarly communication.

References

1. Krafft, D., Cappadona, N., Caruso, B., Corson-Rikert, J., Devare, M., Lowe, B., et al: VIVO: Enabling National Networking of Scientists. In: Proceedings of the WebSci10: Extending the Frontiers of Society On-Line. (April 2010)
2. Burr, W., Dodson, D., Newton, E., Perlner, R., Polk, W., Gupta, S., Nabbus, E.: Electronic Authentication Guideline: NIST Special Publication 800-63-1. National Institute of Standards and Technology. (2011).