# Binding Attributes in the Publish Trust Framework

Hal Warren

American Psychological Association, Washington, DC, USA
hal@apa.org

**Abstract.** In this paper, we describe mechanisms for trusted attribute exchange and binding in the Publish Trust Framework. We first present an overview of a scholarly identity pilot deployed within the Open Identity Exchange (OIX) framework. Then we show how an attribute owner can control the release, retraction and tracking of their attributes using trust standards and open identity protocols.

## 1 Introduction

This paper describes the Publish Trust Framework (PTF), an experiment in digital scholarly identity managed by the American Psychological Association (APA) in partnership with the Human Computer Interaction Lab (HCIL) at the University of Maryland, the InCommon Federation [1], the Open Identity Exchange (OIX) [2], the OpenID Society and the VIVO Development Team at Cornell University [1]. PTF leverages the existing work on trust computation [2] and seeks to discover the most efficient method for the reliable exchange of human online attributes in cyberspace.

Current user-centric approaches to attribute data sharing are based on identity protocols with various degrees of context-dependent privacy requirements and risk controls. [3] describes common federated identity protocols used in account linking and attribute exchange. Today online user accounts are typically bound with an SMTP email address. When a user signs up for a new online service, the email address they give is used to confirm the user through sending a message to the email

[1] http://incommon.org
[2] http://openidentityexchange.org

address which must be answered to activate the account. When this email address is hosted by an institution, it has a higher level of assurance. However, if the service provider does not require identity proofing, there is little or no assurance at all.

The PTF seeks to establish attributes where the strength of the identity of the attribute owner is known through transparent statements about the attribute made manifest at the root of the assertion Uniform Resource Identifier (URI). The objective for PTF is to produce the rapid and reliable exchange of online Trust Attributes through multiple identity providers (IdPs) where trust attributes can be bound to different IdPs and release of those attributes remain in the control of the attribute owner.

We define the Trust Attribute as an assertion by an individual (the attribute owner) backed by a credible party where the URI (as URL) is sourced from that credible party as attribute provider. The individual attribute owner controls release, retraction and tracking of their attributes. Any Trust Attribute can be challenged anonymously or by a known identity.

Next, we describe the structure of the framework and give an overview of a metric for trusted attribute exchange. Finally, we present future work on this project.

## 2 Moving Attributes in the Publish Trust Framework

The Publish Trust Framework is designed to make Identity/Attribute Servers almost as easy to deploy as Web Servers. A complete chain of evidence, from machines, to environment, to network, to the people that have access to the machines, the engineers, developers and administrators will be documented and made transparent through Trusted Parties on published URIs. The PTF provides a registry to make transparent these conditions as URIs expressed on URLs. These assertions of condition are exposed at the root of the attribute. As an example, the URI author.apa.org resolves to HTML for human consumption and RDF-XML or Json for machine consumption. Attributes for machines are formed as semantic triples. This rich assertion allows a single transaction to determine authorship and all co-authors of the individual in question.

Made transparent at the root URI is a description of the reliable party making the claim, the year they were founded and their legal

status, as well as the nature of the attribute being supported and the conditions under which it is presented. Thus, the attribute provider assumes liability for the assertions made. Self-assertions can also be made through the PTF as long as the conditions of the assertion are made transparent at the root URI and consumers of the attribute have the capacity to challenge the claim. This social validation capacity increases the level of trust in the framework.

Attributes that have been proofed to a home address and are backed by a second credible party have higher trust value than most current online social identities. Today our email addresses are the primary means we have to bind identity attributes together online.

The evolving OpenID protocol allows users to login to multiple web services with a single account such as Gmail or a Facebook account. Deployment of the InCommon Federation SAML-based single-sign-on in the PTF allows users to login once and access multiple web services requiring stronger authentication, thus facilitating access to various resources, like telescopes, super-computers and other lab tools that can further research and scientific collaboration.

Attribute binding occurs from stronger assertions. A working draft of the W3C recommendation describes useful behavioral semantics and an extensible method for binding attributes to XML data nodes and evaluating relevant XPath expressions based on the context set by those bindings. [4]

As an example, through the PTF an account without proofing such as Facebook or Gmail can be bound to a proofed account, such as author.apa.org or faculty.utexas.edu. This increases the reliability of the provenance of the Facebook and/or Gmail assertion when sourced from stronger attributes. As attributes coalesce around a specific online identity where all attributes are transparent with machine consumable RDF/Json objects, trustworthiness can be measured and a Trust Factor returned to the consumer. Thus, trust increases and transactional latency and friction are reduced.

In the PTF, attribute owners first verify claims presented by the attribute provider and then control the release of trust attributes. The owner also has the ability to retract and track the usage of their trust attributes by the relying parties.

## 3 The APA Trust Factor = Metric + Variables + Algorithm

We developed a preliminary trust metric for attribute exchange based on the National Institute of Standards and Technology (NIST) Levels of Assurance (LOA) [5].

The APA Trust Metric is anchored at LOA-2 and ranges from 0 to 5 with .1 increments making for a total of 51 possible values. Figure 1 shows the mapping of the APA Trust Factor to NIST LOAs.

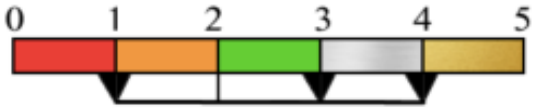


Fig 1. Mapping of the APA Trust Factor metric to NIST Levels of Assurance

The APA Trust Factor metric and variables are transparent to the consumer. The algorithm starts as a computation on the basic conditions of the machine, the environment in which the machine is housed, the network and routers, the people with access to the machine, the transparency of the assertion, and the levels of privacy control provided the attribute owner. This begins as a simple analysis of security elements for the assertion. Over time, as more semantic elements become incorporated with assertions, values for "context" will emerge and can become a part of the factor. We envision the development of an APA Trust Ontology as part of the next phase of this project.

APA Author Attributes are published as Linked Open Data using VIVO as a scholarly identity platform. VIVO produces a rich RDF triplestore for machine analytics aggregated around individual researcher profiles in an organization. The PTF augments the organizational graph with trustworthy provenance metadata and thus represents a trust extension of VIVO.

The Publish Trust Framework is a lightweight method to exchange online attributes within an Open Identity Framework. The PTF uses Internet methods to allow both weak and strong attributes to be exchanged with higher levels of trust. Within the PTF, identity/attribute servers can be deployed with ease. Critical to PTF servers are that the conditions of the machine, the environment, the network and the people are made transparent through URIs which reside at the root of the assertion. These assertions are anonymized by the issuing party to protect security. As an example, author.apa.org (resolving at https://author.apa.org using 256-bit SSL enhanced verification certificate) provides a description of the issuing party and the conditions of the assertion. It also provides a Trustmark with a validation URI from the Identity Server Registry that describes the machine, environment, network and human variables. The assertions for attributes are made transparent at the URI in machine consumable form.

**Attributes with Badges**

Trust attributes will have Trustmarks from other reliable parties that are made transparent at the root URI, such as the Identity Server Registry, an independent auditor, a bank, a locality, the Better Business Bureau, etc. These Trustmarks will always source from the attribute provider thereby giving assurance of validity through a URI.

## 5 Conclusions and Future Work

In this paper, we have presented an overview of the Publish Trust Framework, which uses Semantic Web technologies and trust metrics to reliably bind attributes from authoritative sources.

Attributes often represent communities. From important attributes of employment and credentials to entertainment attributes of a favorite sports team, each has characteristics that help define an individual. When online attributes are aggregated around a single identity, online personality can emerge which then becomes subject to reputation, social acceptance and trustworthiness. Online an individual often has more than one identity, typically one for professional work and one for

family and social connections. Digital identities can also form around hobbies and other special interests.

We deployed a trust framework that binds academic attributes of authorship from publishers to institutions of higher education in semantic payloads with provenance which produce greater trust. The APA Trust Factor will facilitate online trust through analysis of the conditions that make up the underlying assertions of an online identity.

For future work, we intend to use the evolving OpenID Connect protocol to address the issue of disambiguation of scholarly identity in the Publish Trust Framework by binding authorship attributes with established and newly developed author identifiers, including ORCID (Open Researcher and Contributor ID) and ISNI (International Standard Name Identifier).

## 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. Golbeck, J.: Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering. In: Provenance and Annotation of Data, pp. 101-108. (2006) .
3. Maler, E., Reed, D.: The Venn of Identity: Options and Issues in Federated Identity Management, Security & Privacy, IEEE, vol.6, no.2, pp.16-23,(March-April 2008).
4. Boyer, J., The binding attributes module. W3C Working Draft http://www.w3.org/MarkUp/Forms/specs/XForms1.2/modules/instance/bindingAttributes/index-all.html (August 2008)
5. 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).