SAML vs. OpenID

When the Umbrella was built different Web Single Sign-On strategies have been evaluated: OpenID and SAML.

We found that full fledged comparisons between them already existed for similar scenarios:

- http://www.switch.ch/aai/support/faq/SWITCHaai_and_OpenID.html
- http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html

OpenID is “typically internet”, which is good but not for this use case, as only HTTP connections are possible. Also no explicit conformance criteria is defined, which could lead to incompatibility. OpenID lacks a sophisticated trust model – the default trust model is to “trust all end everyone”. User privacy is not explicitly covered in the OpenID specification, which is a very important topic for our use case. As well as all security measures are optional (phishing and man-in-the-middle attacks).

SAML does all of the above right and we found good reasons to stick with SAML. First of all it is free and open source[1]. As a XML-based framework for communicating user authentication, entitlement and attribute information it is foreseen to be extended and custom tailored. SAML is state of the art and is designed by industry experts like EMC, Hewlett Packard, IBM, Microsoft, Nokia, Oracle, SAP, Boeing et. al. It considers user privacy a first-order priority which is crucial for the Umbrella use case. Used by national federations in the (higher) education sector it has shown and proved to work in a real-world environment. Federations across nation boundaries are being worked on. Nevertheless authentication is a dynamic field with ever changing technologies. Using such a standard allows to stay at the cutting edge with a minimum of development efforts.

[1] http://www.shibboleth.net

Topic	**OpenID**	**SAML**
Open Source Implementation Availability:	Open source OpenID implementations are available from several sources.	Open source SAML implementations are available from several sources.
Interoperability Certification and Testing:	There is as yet no testing and certification program for assuring interoperability of implementations.	The SAML specification set includes a conformance specification, and there is at least one formal testing and interoperability certification program.
Specification Style:	The OpenID Authentication specification specifically and concretely addresses Web Single Sign-On (Web SSO) use cases. It is a single monolithic specification binding together the specification of message formats, protocol initiation, identity provider discovery protocol, user identifier definition, and SSO protocol	The SAML specification set modularly specifies two explicitly extensible frameworks, one consisting of security assertions and the other an abstract request-response protocol. These frameworks are then profiled for various usage contexts, one of which is Web SSO, in separate "Profiles" specifications.

	definition.	Other SAML usage contexts include web services security, and SIP identity -- where SAML is profiled in specifications being developed in venues other than OASIS.
Design Center:	The design center of OpenID Authentication is "decentralized" Web SSO, i.e. dynamic interaction between relying parties (RPs) and identity providers (OP/IDPs) without requiring any configuration, setup, prior metadata exchange, or non-vanilla browsers or browser extensions. It can be summarized operationally as "trust and accept all comers". Additionally, it is tacitly intended to be implementable in the "application layer" — meaning, for example, that one should be able to craft simple blog application or wiki application plugins that an end user with the most basic unprivileged hosting account can deploy. Finally, it is also intended to be as trivially implementable as possible. Hence no reliance on a message encoding language, strictly optional security requirements, e.g. message signing, etc. And also there is a minimum of tailorability, and the specification has everything needed for a fairly narrow range of Web SSO use cases baked directly into it, e.g. user identifier treatment and OP/IDP discovery.	SAML's original design center was that of providing a flexible, reusable, secure framework for Web SSO—and security token representation in general—that provides as strong security as possible given the use of HTTP, which is an inherently insecure protocol. Additionally, since a large range of use cases were considered during the design processes of the three SAML versions, it is designed to be highly tailorable in order to meet a wide variety of use cases, and be employable in a variety of protocol contexts. Thus the "core" SAML specification, aka "SAML itself", does not specify use case particulars such as IDP discovery, user identifier treatment, metadata exchange, or even underlying protocol (it can be layered onto or into essentially any other protocol). These particulars are left up to the specification of particular SAML "profiles" and/or "operational modes", which are designed to address specific (sets of) use cases. Although the SAML 2.0 specification set defines several SAML profiles (and associated protocol "bindings") "out of the box" , this does not preclude one from defining new ones, if one's use cases are not met by the existing ones.
Architectural approach:	OpenID 2.0 specifies a concrete web SSO protocol, IDP discovery protocol, user identifier format, an extensibility mechanism (e.g. for attribute exchange), security considerations, and backwards compatibility in a single draft specification.	SAML specifies an abstract extensible security assertion and an abstract extensible request-response protocol via XML schemas, in one specification, the SAML "core". SAML protocol bindings and concrete profiles are defined in further specifications in the specification set, as described below.
End-user Privacy:	End-user privacy is not presently explicitly addressed in OpenID's specification.	End-user privacy is a first-order consideration in SAML 2.0's design.
Security Assertions:	OpenID security assertions are	SAML assertions are explicitly

	comprised of a set of key-value pairs, without explicit message-independent delineation. OpenID does not define an explicitly delineated security assertion object, thus limiting reusability in other protocol contexts.	delineated data objects, with explicitly defined semantics, are explicitly extensible, and feature the capability to represent unambiguous claims about a subject.
Message Structure:	OpenID messages are comprised of simple sets of key-value (aka name-value) pairs, and thus representation of hierarchically-related data, and/or multi-valued keys, is not directly supported.	SAML assertions and protocol messages are explicitly extensible and tailorable, thus facilitating reuse in addressing new and different use cases, e.g. web services security.
Profilability:	OpenID as-specified is not explicitly profilable. The OpenID Authentication specification constitutes one concrete Web SSO "profile".	SAML is explicitly profilable. This is a consequence of both the design center, the specification set style, and the explicit use of an extensible encoding language (XML). Note that to conduct a "concrete" comparison of Web SSO capabilities and approach of SAML and OpenID, one needs to compare the "SAML Web Browser SSO Profile" with the OpenID specification, rather than comparing OpenID Authentication with SAML as a whole.
Extensibility:	OpenID is rudimentally extensible in that it allows for arbitrary additional key-value pairs to be embedded in messages along with an overall "namespace" key, serving to identify the extension's set of keys. Essentially, this allows one to use the HTTP-redirect-based message exchange (between the RP and the OP/IDP) machinery to convey arbitrary "messages" consisting of differing sets of key-value pairs. This can be used, for example, to effect attribute exchange.	SAML is explicitly extensible in several fashions, including the protocol message layer, the assertions themselves, and in terms of the design modularity — one can relatively easily craft new "bindings" and "profiles" if existing ones do not meet one's needs.
Trust and Security Considerations:	OpenID's implicit trust framework and security considerations are not thoroughly examined.	The SAML specification set includes a thorough analysis of the SAML profiles' security considerations. The SAML trust framework depends upon the specific context of use, and thus the particular SAML profile being employed. This is examined for the SAML profiles included in the SAML specification set.
Protocol bindings:	OpenID specifies two bindings to HTTP POST and HTTP GET (and requisite responses) messages. The former is intended for so-called "direct" interactions between	Protocol bindings of abstract request-response protocol messages to concrete underlying protocols, e.g. HTTP and SOAP, are specified in the ""SAML

	system entities (i.e. not redirected), and the latter are explicitly defined as being redirected through the user agent. The specification does not provide guidance with respect to the creation of any other bindings.	Bindings" specification. All of HTTP POST, HTTP redirect, SOAP-over-HTTP, reverse SOAP-over-HTTP ("PAOS"), SAML Artifact, and SAML URI bindings are specified.
Metadata support:	OpenID relies on XRDS documents, which can be found by resolving an XRI , for what is essentially "service metadata" in SAML terminology. Additionally, OpenID relies upon establishing so-called "associations" for exchanging keying material between an RP and an OP/IDP.	SAML metadata, e.g. for identity providers and relying parties (aka service providers), are defined in the "SAML metadata" specification
Conformance criteria:	The OpenID specification set does not explicitly define conformance criteria at this time. Rather it is implicit in the specification(s).	Conformance criteria and the specification roadmap are given in the "SAML conformance" specification.
Security considerations:	Security considerations are nominally discussed. An incomplete security profiles draft spec by an individual contributor, remains at version -01, from Sep-2006.	Security considerations are presented and examined in the "SAML sec considerations" specification.

Table 1: Comparison Table of Features. Source: http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html