The Emerging JSON-Based Identity Protocol Suite

Michael B. Jones

mbj@microsoft.com – http://self-issued.info/

April 27, 2011

Submission to W3C Workshop on Identity in the Browser

Abstract

A new set of open identity protocols is emerging that utilizes JSON data representations and simple REST-based communication patterns. These protocols and data formats are intentionally designed to be easy to use in browsers and modern web development environments.

1. Introduction

Achieving interoperable identity systems requires agreement on data representations and protocols among the participants. While there are several suites of successful interoperable identity data representations and protocols, including Kerberos [Neuman & Ts'o 94], X.509 [PKIX 05], SAML 2.0 [Cantor 05], WS-* [WS-Security 04, WS-Trust 09, WS-SecurityPolicy 09], and OpenID 2.0 [OpenID 07], they have used data representations that have limited or no support in browsers and modern web development environments, such as ASN.1 [ITU 02], XML [XML 08], or custom data representations.

A new set of open identity protocols is emerging that utilizes JSON [RFC 4627] data representations and simple REST-based [Fielding 00] communication patterns. These protocols and data formats are intentionally designed to be easy to use in browsers and modern web development environments, which typically include native JSON support. This paper surveys a number of the emerging open JSON-based identity protocols. It concludes by discussing how they can facilitate the emergence of identity in the browser.

2. The Emerging JSON-Based Identity Protocol Suite

This section provides an overview of a set of open, JSON-based identity protocols that are being collaboratively developed by members of the identity community. These protocols are designed to work together to enable open, interoperable, claims-based identity, authentication, and authorization services to be built for the Web.

2.1. JSON Web Token, Signature, Encryption, and Key Specifications

The ability to produce signed and optionally encrypted security tokens containing claims is fundamental to interoperable identity protocols. This family of specifications meets this need.

2.1.1. JSON Web Token (JWT)

A JSON Web Token (JWT) [JWT 11] is a means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is digitally signed using a JSON Web Signature (JWS) [JWS 11] and optionally encrypted using JSON Web Encryption (JWE) [JWE 11]. This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Several independent and interoperable implementations of JWTs already exist. JWT has been submitted as an Internet Draft.

The suggested pronunciation of JWT is the same as the English word “jot”.

2.1.2. JSON Web Signature (JWS)

JSON Web Signature (JWS) [JWS 11] is a means of representing signed content using JSON data structures. Complementary encryption capabilities are described in the closely related JSON Web Encryption (JWE) specification. This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Several independent and interoperable implementations of the JWS spec already exist. JWS has been submitted as an Internet Draft.

2.1.3. JSON Web Encryption (JWE)

JSON Web Encryption (JWE) [JWE 11] is a means of representing encrypted content using JSON data structures. This specification builds upon the signature capabilities described in the closely related JSON Web Signature (JWS) [JWS 11] specification. It is likely that this specification will incorporate capabilities first described in the JavaScript Message Security Format [JSMS 11] draft.

2.1.4. JSON Web Key (JWK)

A JSON Web Key (JWK) [JWK 11] is a JSON data structure that represents a set of public keys. The JWK format is used to represent bare keys; representing certificate chains is an explicit non-goal of this specification. JSON Web Keys are referenced in JSON Web Signatures (JWSs) [JWS 11] using the `jku` (JSON Key URL) header parameter.

2.2. Simple Web Discovery (SWD)

Simple Web Discovery (SWD) [SWD 10] defines an HTTPS GET based mechanism to discover the location of a given type of service for a given principal starting only with a domain name. SWD has been submitted as an Internet Draft.

2.3. OAuth 2.0 Specifications

The OAuth 2.0 family of specifications enable scoped authorization of third-party applications to HTTP-based services to occur without releasing end-user credentials to those applications. The OAuth specifications use JSON data structures to represent structured data.

2.3.1. The OAuth 2.0 Authorization Protocol

The OAuth 2.0 authorization protocol [OAuth 11a] enables granting third-party applications limited access to an HTTP service on behalf of an end-user by orchestrating an approval interaction between the end-user and the HTTP service. This specification is nearing approval as an RFC.

2.3.2. The OAuth 2.0 Protocol: Bearer Tokens

OAuth enables clients to access protected resources by obtaining an access token, rather than using the resource owner's credentials. Tokens are issued to clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server. This specification [OAuth 11b] describes how to make protected resource requests when the OAuth access token is a bearer token. This specification is nearing approval as an RFC.

2.3.3. JSON Web Token (JWT) Bearer Profile for OAuth 2.0

This specification [OAuth 11c] defines the use of a JSON Web Token (JWT) bearer token as a means of requesting an OAuth 2.0 access token. This specification has been submitted as an Internet Draft.

2.4. OpenID Artifact Binding/Connect Specifications

The OpenID Artifact Binding/Connect (OpenID AB/C)[1] [OpenID 11a, OpenID 11b] specifications enable Facebook Connect [Facebook 08] like functionality from an open set of identity providers while also addressing some of the limitations of the OpenID 2.0 [OpenID 07] specifications. These specifications build upon OAuth 2.0, JWT, JWS, JWE, and SWD. An explicit design point for the OpenID AB/C protocols is enabling agents working on users' behalf, including browsers, to mediate users' identity interactions. These protocols are in active development by a diverse and influential set of individuals within the identity community.

3. Conclusions

A rich suite of complimentary and interoperable identity protocols using JSON data structures and RESTful communication patterns is being developed. These protocols retain much of the semantic richness of previous standards, while being easier to use across a broad range of web development tools and browsers.

These protocols are being designed with an explicit awareness of the capabilities of modern browsers, including JSON support. Indeed, the designers believe that the emerging suite of JSON-based identity protocol represents a useful and appropriate set of building blocks for enabling identity in the browser.

References

[Cantor 05] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* OASIS Standard, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[1] Almost certainly not the final branding for these specifications.

[Facebook 08] *Facebook Connect*, May 2008. http://developers.facebook.com/blog/post/108.

[Fielding 00] Representational State Transfer (REST): Chapter 5 of *Architectural Styles and the Design of Network-based Software Architectures*, 2000. http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm.

[ITU 02] ITU-T X.690, OSI networking and system aspects – Abstract Syntax Notation One (ASN.1): *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, July 2002. http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf.

[JSMS 11] *JavaScript Message Security Format*, March 2011. http://www.ietf.org/id/draft-rescorla-jsms-00.txt.

[JWE 11] *JSON Web Encryption (JWE)*, March 2011. http://self-issued.info/docs/draft-jones-json-web-encryption.html.

[JWK 11] *JSON Web Key (JWK)*, April 2011. http://self-issued.info/docs/draft-jones-json-web-key.html.

[JWS 11] *JSON Web Signature (JWS)*, March 2011. http://self-issued.info/docs/draft-jones-json-web-signature.html.

[JWT 11] *JSON Web Token (JWT)*, March 2011. http://self-issued.info/docs/draft-jones-json-web-token.html.

[Neuman & Ts'o 94] B. Clifford Neuman and Theodore Ts'o (September 1994). Kerberos: An Authentication Service for Computer Networks. *IEEE Communications* **32** (9): 33–8.

[OAuth 11a] *The OAuth 2.0 Authorization Protocol*, April 2011. http://tools.ietf.org/html/draft-ietf-oauth-v2-15.

[OAuth 11b] *The OAuth 2.0 Protocol: Bearer Tokens*, March 2011. http://self-issued.info/docs/draft-ietf-oauth-v2-bearer.html.

[OAuth 11c] *JSON Web Token (JWT) Bearer Profile for OAuth 2.0*, March 2011. http://self-issued.info/docs/draft-jones-oauth-jwt-bearer.html.

[OpenID 07] *OpenID Authentication 2.0*, December 2007. http://openid.net/specs/openid-authentication-2_0.html.

[OpenID 11a] *OpenID Connect Core 1.0*, January 2011. http://openid4.us/specs/ab/openid-connect-core-1_0.html.

[OpenID 11b] *OpenID Connect Artifact Binding 1.0*, January 2011. http://openid4.us/specs/ab/openid-connect-ab-1_0.html.

[PKIX 05] *Public-Key Infrastructure (X.509) (pkix)*, December 2005. http://www.ietf.org/html.charters/pkix-charter.html.

[RFC 4627] D. Crockford, *The application/json Media Type for JavaScript Object Notation (JSON)*, July 2006. http://tools.ietf.org/html/rfc4627.

[SWD 10] *Simple Web Discovery (SWD)*, October 2010. http://self-issued.info/docs/draft-jones-simple-web-discovery.html.

[WS-Security 04] *Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)*, OASIS Standard, March 2004. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

[WS-SecurityPolicy 09] *WS-SecurityPolicy 1.3*, OASIS Standard, February 2009. http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.3/os/ws-securitypolicy-1.3-spec-os.html.

[WS-Trust 09] *WS-Trust 1.4*, OASIS Standard, February 2009. http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.html.

[XML 08] *Extensible Markup Language (XML) 1.0 (Fifth Edition)*, W3C Recommendation, November 2008. http://www.w3.org/TR/2008/REC-xml-20081126/.