TOPIC

IDENTITY MANAGEMENT

PRIVACY BY DESIGN AND THE ONLINE LIBRARY

FROM THE LIBRARY OF CONGRESS TO THE LIBRARY OF ME

THE INTENTION PUBLISHING ECONOMY: WHEN PATRONS TAKE CHARGE

A JSON-BASED IDENTITY PROTOCOL SUITE
Achieving interoperable digital 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, X.509, SAML 2.0, WS-* and OpenID 2.0, they have used data representations that have limited or no support in browsers, mobile devices, and modern Web development environments, such as ASN.1, XML or custom data representations.

A new set of open digital identity standards have emerged that utilize JSON data representations and simple REST-based communication patterns. These protocols and data formats are intentionally designed to be easy to use in browsers, mobile devices, and modern Web development environments, which typically include native JSON support. This paper surveys a number of these open JSON-based digital identity protocols and discusses how they are being used to provide practical interoperable digital identity solutions.

THE EMERGING JSON-BASED IDENTITY PROTOCOL SUITE

This section provides an overview of a set of open, JavaScript Object Notation (JSON)-based digital 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.

JSON Web Token, Signature, Encryption, Key, and Algorithms Specifications

The ability to produce signed and optionally encrypted security tokens containing claims is fundamental to interoperable identity protocols. A security token is a cryptographically secured set of statements made by an issuer about a subject that can be used by the intended recipient to make trust decisions about the subject. Claims are the individual statements in the security token about the subject made by the issuer. This family of JSON-based specifications meets this need.
**JSON Web Token (JWT)**

A JSON Web Token (JWT) 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 JSON Web Signature (JWS) and optionally encrypted using JSON Web Encryption (JWE). Using a JWT enables the issuer of a token to make statements about the subject of the token to an intended audience in a way receivers can verify that they were made by the issuer. This capability is fundamental to digital identity systems. For instance, OpenID Connect uses a JWT issued by the identity provider, whose audience is the relying party, to make authoritative claims that a particular user (the subject of the JWT) has logged in at the identity provider.

This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Over a dozen independent and interoperable implementations of JWTs are known to exist at this point—many of them in production use. The IETF OAuth Working Group has requested publication of JWT as a Request for Comment (RFC)—an IETF standard.

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

**JSON Web Signature (JWS)**

JSON Web Signature (JWS) 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. For instance, the JSON Web Token (JWT) specification uses JWS for the issuer to sign JWTs.

This specification was developed collaboratively based upon inputs from a number of independently developed precursor JSON token, signing, and encryption specifications. Over a dozen independent and interoperable implementations of the JWS specification are known to exist at this point, many of them in production use. The IETF JSON Object Signing and Encryption (JOSE) working group has requested publication of JWS as an RFC—an IETF standard.

**JSON Web Encryption (JWE)**

JSON Web Encryption (JWE) is a means of representing encrypted content using JSON data structures. This specification complements the signature capabilities described in the closely related JSON Web Signature (JWS) specification. Encryption enables participants to pass confidential messages between themselves.

Several independent and interoperable implementations of the JWE specification are known to exist at this point, many of them in production use. Like JWS, publication of JWE has been requested as an RFC.
A rich suite of complementary and interoperable digital identity standards using JSON data structures and RESTful communication patterns has emerged and is in increasingly widespread use. 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 platforms.
OpenID Connect Specifications
The OpenID Connect specifications enable Facebook Connect-like functionality from an open set of identity providers while also addressing some of the limitations of the OpenID 2.0 specifications. Put another way, it enables you to log into a relying party using a digital identity at an identity provider of your choice. These specifications build upon OAuth 2.0, JWT, JWS, JWE, JWK, JWA, and WebFinger. An explicit design point for the OpenID Connect protocols is enabling agents working on users’ behalf, including browsers and mobile applications, to mediate users’ identity interactions.

The OpenID Connect specifications were completed in February 2014. They are in production use by many organizations, including Google, Microsoft, Yahoo! Japan, Deutsche Telekom, Ping Identity, and Salesforce. For instance, when you’re signing into Google+ or using Azure Active Directory, you’re actually using OpenID Connect.

CONCLUSIONS
A rich suite of complementary and interoperable digital identity standards using JSON data structures and RESTful communication patterns has emerged and is in increasingly widespread use. 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 platforms.

These protocols are being designed with an explicit awareness of the capabilities of modern browsers and Web development tools, including JSON support. Indeed, the designers believe that the already widespread adoption of these JSON-based digital identity standards demonstrates their usefulness for providing practical interoperable digital identity solutions.

Michael B. Jones (mbj@microsoft.com) is an Identity Standards Architect at Microsoft and the author of the blog Self-Issued: Musings on Digital Identity (http://self-issued.info/).

REFERENCES