Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 8, 2016

P. Hallam-Baker
Comodo Group Inc.

March 7, 2016

JSON Web Service Binding Version 1.0
draft-hallambaker-json-web-service-02

Abstract

The JSON Web Binding (JWB) describes a standardized approach to implementing Web Services. Services are advertised using the DNS SRV and HTTP Well Known Service conventions. Messages may be authenticated or authenticated and encrypted at the message layer in addition to any transport and/or network layer security. Service messages are encoded in JSON using Internet time format for Date-Time fields and Base64urlencoding for binary objects.

This document specifies Version 1.0 of JWB which uses HTTP/1.1 for transport. Use of the multiple stream capabilities of HTTP version 2 is outside the scope of this document.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 8, 2016.

Copyright Notice

1. Introduction

The JSON Web Binding (JWB) specifies one approach to using DNS Discovery [RFC1035], the HTTP [RFC7230] protocol and the JSON data encoding [RFC7159] in a Web Service.

JWB is not the only approach possible, but developing a standard means making choices that don't matter to developers that build on it. While there are infinitely many ways that a Web Service might employ HTTP and JSON to implement a Web Service, a client and a server can only interoperate if they both agree to use the same one.

Discovery Beginning with a DNS address of the service (e.g. example.com), the client identifies a specific HTTP URL at which to access the service. The DNS SRV record [RFC2782] and Well Known Service [RFC5785] mechanisms are used for this purpose.

Authentication and Encryption Web Services MAY require authentication and encryption services at the message level even if transport layer security (e.g. TLS [RFC5264]) is used. Use of such enhancements is signaled using the HTTP Content-Encoding header.

Content Mapping The mapping of data types described in the specification (integer, string, etc.) to JSON data types. [RFC3339] Date time encoding and BASE64-url encoding [RFC4648] are used to map date-time and binary data types to JSON encoding values.

A key architectural principle that guides the design of JWB is that the Web Service application should be as independent of the HTTP presentation layer as is possible. Thus:

Message semantics are not affected by HTTP headers or the request line URL.

The use of HTTP response codes is limited to reporting errors and warnings that arise from the HTTP transport.

If message layer authentication or authenticated encryption are used, this is applied within the HTTP content payload and not through a combination of payload and header data.

This specification describes a mechanism for accessing a collection of hosts as a single undifferentiated service with provision for load balancing and fault tolerance. This has important consequences for state management. Web Services typically involve some form of stateful interaction or real world side effect. Otherwise, it is likely that the Web Service would be better written as a traditional Web interaction mapping the stateless resources to URIs.

The mechanism described in this specification is intended for the initial discovery of a host with which to engage in a Web Service transaction which may or may not consist of a series of message exchanges. Since sharing state between hosts supporting a virtual service requires resources and typically introduces latency, a service specification MAY require that a transaction begun on one host be completed with the same host and the time period in which a transaction that is accepted by one host will be regarded as 'final' by the virtual service.

For example, a file upload protocol for a photograph sharing service might have separate messages for checking that there is space to store the photograph 'Check', uploading the file 'Store' and reporting that the data is safely stored at multiple locations. When responding to the Check command, the host is reporting that there is space at that local node. It is obviously undesirable for a client to verify that host1 has enough space to store the file and then attempt to upload the file to host2. Equally, having uploaded the file to host1, it might be minutes, hours or even days before the photograph could be retrieved through host2. Such questions are left for the Web Service protocol designer to address.

2. Definitions

2.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

3. Service Discovery

Service discovery is the process of resolving the address of a Web Service to a Web Service Endpoint, a URI [RFC3986] at which the service is provided.

A JWB Web Service is specified by giving the DNS Address of the service <domain>, and Well Known Service name <service>.

3.1. Host Identification

The first step in service discovery is to resolve the <domain> and <service> identifiers to the IP address of a host that provides that service.

3.1.1. SRV Lookup

A client attempting to connect to the service first attempts to locate an SRV record [RFC2782] for the specified service:

_<service>._tcp._<domain> SRV <priority> <weight> <port> <mapping>

Where <priority> and <weight> are the SRV priority and weight parameters specified in [RFC2782], <port> is the TCP port number and <mapping> is the DNS name of the host for which the service advertisement is made. Standard A/AAAA/CNAME resolution is used to obtain the IP address of the host from <mapping>.

If a match is found, the client uses the mechanism specified in [RFC2782] to choose hosts and attempts to contact each host in turn until a successful HTTP connection is established or the maximum number of attempts threshold is reached.

3.1.2. DNS Fallback

Despite the fact that SRV records have been a part of the DNS standard for 20 years, it is not uncommon for network intermediaries to implement SRV record resolution incorrectly or block it entirely.

If no SRV record is found, a client MAY perform fallback discovery if explicitly authorized to do so by the corresponding Web Service protocol specification. The client attempts to connect to the host <service>.<domain> using the standard A/AAAA/CNAME resolution rules to obtain the IP address of the host.

3.2. HTTP host processing

Having identified the IP address, the client performs a HTTP or HTTPS Web Service POST request at the default Web Service Endpoint specified by the Well Known Service name and the original DNS address of the service.

http://<domain>:<port>/.well-known/<service>

Note that a given host MAY provide multiple instances of a Web Service under different discovery addresses. Therefore it is essential to use the original <domain> value rather than the <mapping> returned in the SRV record.

3.2.1. Use of TLS transport

The use of TLS transport is indicated by the SRV port number as follows:

If the SRV port number is 80, 8000, 8080 or greater than 32,767 HTTP over TCP is used.

Otherwise HTTP over TLS Transport (HTTPS) is used.

If an authenticated DNS resolution protocol (e.g. DNSSEC [RFC4033]) is used to resolve the SRV record, these rules permit deployments to achieve 'secure on first contact' transport security without the need to resolve additional records (e.g. TLSA [RFC6698]. Note however that while the use of TLS is mandated, the criteria for evaluating the TLS certificate chain presented by the server is left to local site policy.

A service presented on a port for which HTTP is indicated MAY specify a redirect to require use of HTTPS protocol.

3.2.2. Fallback Processing Rules

If a client's attempt to connect to a host selected from an SRV connection redirection results in a HTTP (3xx), Client error (4xx) or Server error (5xx) code, the client MUST process the HTTP error response and not simply attempt a connection to a different host. If a client request is rejected for lack of authentication (511) or because the request is too large (413) at one host, the client should assume that the request will be rejected for the same reason at another. If the attempt to create a TCP connection fails or the server returns Service Unavailable (503), the client MAY use the SRV fallback rules to select an alternative host.

3.2.3. Service Continuation

Once the initial service discovery mechanism has been used to establish contact with a host, the service protocol MAY specify that further interactions be directed to another host and/or using a different protocol. Such mechanisms are outside the scope of this specification.

3.3. Example

The Mathematical Mesh has the Well Known Service name of 'MMM'. Accounts used in the Mathematical Mesh follow the [RFC5822] format of <user>@<domain>.

Alice has the account alice@example.com and the DNS configuration file for example.com has the following entries:

```
_mmm._tcp.example.com SRV host1.example.com 0 10 80 host1.example.com
_mmm._tcp.example.com SRV host2.example.com 0 40 80 host2.example.com
mmm.example.com       CNAME host3.example.com
host1.example.com     A 10.0.1.1
host2.example.com     A 10.0.1.2
host3.example.com     A 10.0.1.1
host3.example.com     A 10.0.1.2
```

The client attempts to resolve the address alice@example.com as follows:

Client attempts to resolve SRV record for _mmm._tcp.example.com

DNS resolver returns two entries.

Client makes a random selection between host1 (20% weighting) and host2 (80% weighting). Chooses host1.

Client resolves A/AAAA for host1.example.com

DNS resolver returns 10.0.1.1

Client attempts to POST Web Service request to http://example.com/.well-known/mmm at host address 10.0.1.1

The host at 10.0.1.1 returns 503 Service Unavailable

Client resolves A/AAAA for host2.example.com

DNS resolver returns 10.0.1.2

Client attempts to POST Web Service request to http://example.com/.well-known/mmm at host address 10.0.1.2

Request succeeds, session proceeds.

If the same client is used in a network location where the SRV record resolution fails due to a faulty firewall configuration, the resolution proceeds as follows:

Client attempts to resolve SRV record for _mmm._tcp.example.com

DNS resolver returns 'not found'

Client attempts to resolve A and AAAA record

DNS resolver returns 10.0.1.1, 10.0.1.2

Client makes a random selection between 10.0.1.1 (50% weighting) and 10.0.1.2 (50% weighting). Chooses host1.

Client attempts to POST Web Service request to http://example.com/.well-known/mmm at host address 10.0.1.1

The host at 10.0.1.1 returns 503 Service Unavailable

Client attempts to POST Web Service request to http://example.com/.well-known/mmm at host address 10.0.1.2

Request succeeds, session proceeds.

Note that the main difference between these two scenarios is that the use of the SRV record allows the service configuration to account for load balancing with tiers of fallback support while the use of round robin A/AAAA records does not.

4. HTTP Messages

JWB messages are exchanged as HTTP POST transactions. Support for and use of HTTP/1.1 [RFC7230] is REQUIRED unless otherwise specified by the Web Service Specification.

While the use of HTTP/2 [RFC7540] offers the potential benefit of multiple concurrent transaction streams, the means of making use of such capabilities is outside the scope of JWB v1.0 but is likely to be the main incentive for defining a revision.

In contrast to other approaches to the design of Web Services, the only use made of the HTTP transport is to distinguish between different services on the same host using the Host header and .well-known convention and for message framing.

In particular no use is made of the URI request line to identify commands, nor are the caching or proxy capabilities of HTTP. One of the main design objectives of JWB is to enable message level authentication. Since HTTP headers are mutable and may be changed by intermediaries, any attempt to make use of HTTP features requires a mechanism to canonicalize or duplicate the headers. Furthermore, the

implementation of authentication and encryption features at the message level is liable to be incompatible with the HTTP caching model and any attempt to implement caching is moot when TLS is in use.

4.1. Request

The HTTP request MAY contain any valid HTTP header specified in [RFC7230].

Request Line URI /well-known/<service>

Request Line Method POST

Host: Header <domain>

Content-Encoding As specified in section yy below.

Content-Type As specified in section zz below.

Content-Length or Transfer-Encoding As specified in [RFC7230].

Payload The content payload as specified in section XX below.

Example: The HTTP request for the mmm service in the previous example would be:

```
POST /.well-known/mmm HTTP/1.1
Host: example.com
Content-Type: application/json
Content-Length: 16

{ ?hello? : {} }
```

4.2. Response

The response MAY contain any HTTP response header. However since JWB services do not make use of HTTP caching and messages are not intended to be modified by HTTP intermediaries, only a limited number of headers have significance.

Response Code The HTTP response code. This is processed as described in section zz below.

Content-Type As specified in section zz below.

Content-Length or Transfer-Encoding As specified in [RFC7230].

Cache-Control Since the only valid HTTP method for a JWB request is POST, JWB responses are not cacheable. The use of the cache-control header is therefore unnecessary. However experience suggests that reviewers find it easier to understand protocol specifications if they are reminded of the fact that caching is neither supported nor desired.

Example: The HTTP response for the mmm service in the previous example would be:

```
HTTP/1.1 200 OK
Content-Type: application/json
Connection: keep-alive
Cache-Control: no-store
Content-Length: 43

{ ?hello-response? : { ?Version? : ?1.0? }}
```

5. Error handling and response codes

A JWB Web Service is effectively using a three layer protocol stack with the potential for an error to occur at any of the three layers:

Transport Layer

HTTP Layer

Web Service Layer

Services SHOULD always attempt to return error codes at the highest level possible. However it is clearly impossible for a connection that is refused at the Transport layer to return an error code at the HTTP layer. It is however possible for a HTTP layer error response to contain a content body.

In the case that a JWB response contains both a HTTP response code and a well formed JWB payload containing a response, the JWB payload response SHALL have precedence.

6. Content Encoding

The HTTP Content-Encoding header specifies transformations performed on the content before the HTTP Transfer encoding was applied. This is commonly used for specifying compression. In JWB the Content-

Encoding header MAY be used to specify that the content that follows contains a payload that is either authenticated [RFC7515] or authenticated and encrypted [RFC7516] using the JOSE specification.

6.1. Direct Encoding

If the Content-Encoding header is absent or empty, the HTTP content is the message payload as specified by the Content-Type header.

6.2. Content-Encoding: jose-jwb

The Content-Encoding type jose-jwb is a serialization format for JSON Web Signature and JSON Web Encryption objects. Each message consists of the following sequence:

Preamble: A JSON object in UTF-8 encoding

ASCII Record Separator Character (%x1E)

Payload

ASCII Record Separator Character (%x1E)

Postscript: A JSON object in UTF-8 encoding

The payload data consists of all the data that appears between the first and the last occurrence of the record separator character %x1E in the HTTP content. Since the UTF-8 encoding does not permit the octet %0x1E to occur within a well formed JSON object, the use of this character as a record separator is unambiguous even if the character occurs within the payload (as is possible with a binary content-type or if the payload is encrypted).

The contents of the Preamble, Payload and Postscript vary according to whether the message is authenticated or authenticated and encrypted.

6.3. Authenticated

Authenticated messages are signed using Jose Web Signature [RFC7515]. The Preamble, Payload and Postscript are formed as follows:

Preamble A JSON Object containing the JWS Protected Header

Payload The binary data over which the signature value is calculated

Postscript The JWS Signature header

Note that a jsoe-jwb message is only permitted to have a single header and there is no provision for providing data that is not integrity protected.

6.4. Authenticated Encryption

Authenticated messages are signed using Jose Web Signature [RFC7515]. The Preamble, Payload and Postscript are formed as follows:

Preamble A JSON Object containing the JWS Protected Header

Payload The binary data over which the signature value is calculated

Postscript The JWS Signature header

Note that a jsoe-jwb message is only permitted to have a single header and there is no provision for providing data that is not integrity protected.

7. Content Type

The Content Type header specifies the plaintext payload media type as specified in [RFC6838].

For version1.0 of this specification, the only supported payload media type is application/json as specified in [RFC7159].

Future versions of this specification may include support for binary encodings such as JSON-B [draft-hallambaker-jsonbcd] and/or CBOR [rfc7049].

8. JSON Data Bindings

Note that this is the only part of this specification that is strictly limited to JSON encoding. The rest of the specification is equally applicable to Web Services using XML and/or CBOR encoding.

8.1. Request Message

Each JWBv1.0 request contains exactly one Web Service Command. [Future versions MAY specify a mechanism that permits multiple commands to be sent in parallel]

The request payload contains a JSON object that contains exactly one member whose name is the name of the command that is requested and whose value is an object that contains the command parameters (if any).

```
{ ?hello? : {} }
```

8.2. Response Message

The response payload contains a JSON object that contains the members specified by the Web Service specification.

Future versions of this specification MAY reserve particular fields in the response payload for particular purposes (e.g. returning status values).

```
{ ?hello-response? : { ?Version? : ?1.0? }}
```

8.3. Data Fields

JSON was originally developed to provide a serialization format for the JavaScript programming language [ECMA-262]. While this approach is generally applicable to the type systems of scripting programming languages, it is less well matched to the richer type systems of modern object oriented programming languages such as Java and C#. Moreover

Working within a subset of the capabilities of JSON allows a Web Service protocol to be accessed with equal ease from either platform type. In particular the following capabilities of JSON are avoided:

The ability to use arbitrary strings as field names.

The use of JSON objects to define maps directly

The following data field types are used:

Integer Integer values are encoded as JSON number values.

String Test strings are encoded as JSON text strings.

Boolean Boolean values are encoded as JSON 'false', 'true' or 'null' tokens according to value.

Sequence Sequences of data items that are encoded as JSON arrays

Object of known type Objects whose type is known to the receiver are encoded as JSON objects

Object of variable type Objects whose type is not known to the receiver are encoded as JSON objects containing a single field whose name describes the type of the object value and whose value contains the value.

Binary Data Byte sequences are converted to BASE64-url encoding [RFC4648] and encoded as JSON string values.

Date Time Date Time values are converted to Internet time format as described in [RFC3339] and encoded as JSON string values.

9. Security Considerations

A fuller treatment of the security considerations will follow.

9.1. Integrity

9.1.1. DNS Spoofing

9.1.2. TLS Downgrade

9.1.3. TLS Service Impersonation

9.1.4. Request Replay Attack

9.1.5. Response Replay Attack

9.2. Confidentiality

9.2.1. Side Channel Attack

9.2.2. Session Key Leakage

10. IANA Considerations

The following registrations are required:

HTTP Content Coding Registry jose-jwb

Well-Known URIs /.well-known/srv/

[Or change registry to FCFS]

11. References

11.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987.

[RFC7230] Fielding, R. and J. Reschke, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014.

[RFC7159] Bray, T., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, DOI 10.17487/RFC2782, February 2000.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010.

[RFC5264] Niemi, A., Lonnfors, M., and E. Leppanen, "Publication of Partial Presence Information", RFC 5264, DOI 10.17487/RFC5264, September 2008.

[RFC3339] Klyne, G. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, DOI 10.17487/RFC3339, July 2002.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, DOI 10.17487/RFC3986, January 2005.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015.

[RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", BCP 13, RFC 6838, DOI 10.17487/RFC6838, January 2013.

[RFC5822] "[Reference Not Found!]".

11.2. Informative References

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015.

[draft-hallambaker-jsonbcd] "[Reference Not Found!]".

[ECMA-262] "[Reference Not Found!]".

Author's Address

Phillip Hallam-Baker
Comodo Group Inc.

Email: philliph@comodo.com