Open Retailing API Implementation Guide: Transport Alternatives

February 3, 2020

Version 1.1.1

Document Summary

This document describes the Open Retailing (fuel retailing and convenience store) transport layer alternatives for RESTful web services carrying JSON based APIs.

Contributors

Axel Mammes, OrionTech
Gonzalo Gomez, OrionTech
Linda Toth, Conexxus
David Ezell, Conexxus
John Carrier, IFSF

This document was reviewed and approved by the Joint IFSF and Conexxus Application Programming Interface Work Group and the Technical Advisory Committee within Conexxus.

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
3 February 2020	V1.1.1	Linda Toth, Conexxus	Changed fuel retailing to open retailing.
28 July 2019	V1.1	John Carrier, IFSF	Update to version 1.1 for publication.
15 July 2019	Final Draft V1.1	Linda Toth, Conexxus	Accepted changes, cleaned up formatting.
8 July 2019	V1.0.4	David Ezell, Conexxus	Clean up wording per conversation with Linda Toth.
5 July 2019	V1.0.3	Linda Toth, Conexxus	Reformatted to joint format
24 June 2019	V1.0.2	John Carrier, IFSF	Title changed to Part 4-03 API Implementation Guide – Transport Alternatives.
12 May 2019	V1.0.1	John Carrier, IFSF	Update to include approval from Conexxus Technical Advisory Committee.
28 May 2019	V1.0	John Carrier, IFSF	First published version.
30 April 2019	Final Draft v0.1	John Carrier, IFSF David Ezell, Conexxus Gonzalo Gomez, OrionTech	Final draft for approval.
17 April 2019	Draft V0.1	John Carrier, IFSF	Initial Draft for API WG Review based on V0.3 of the API Paper of the same name. The Joint API WG required the paper to become a full Standard.

Copyright Statement

The content (content being images, text or any other medium contained within this document which is eligible of copyright protection) are jointly copyrighted by Conexxus and IFSF. All rights are expressly reserved.

IF YOU ACQUIRE THIS DOCUMENT FROM IFSF. THE FOLLOWING STATEMENT ON THE USE OF COPYRIGHTED MATERIAL APPLIES:

You may print or download to a local hard disk extracts for your own business use. Any other redistribution or reproduction of part or all of the contents in any form is prohibited.

You may not, except with our express written permission, distribute to any third party. Where permission to distribute is granted by IFSF, the material must be acknowledged as IFSF copyright and the document title specified. Where third party material has been identified, permission from the respective copyright holder must be sought.

You agree to abide by all copyright notices and restrictions attached to the content and not to remove or alter any such notice or restriction.

Subject to the following paragraph, you may design, develop and offer for sale products which embody the functionality described in this document.

No part of the content of this document may be claimed as the Intellectual property of any organisation other than IFSF Ltd, and you specifically agree not to claim patent rights or other IPR protection that relates to:

a) the content of this document; or
b) any design or part thereof that embodies the content of this document whether in whole or part.

For further copies and amendments to this document please contact: IFSF Technical Services via the IFSF Web Site (www.ifsf.org).

IF YOU ACQUIRE THIS DOCUMENT FROM CONEXXUS, THE FOLLOWING STATEMENT ON THE USE OF COPYRIGHTED MATERIAL APPLIES:

Conexxus members may use this document for purposes consistent with the adoption of the Conexxus Standard (and/or the related documentation); however, Conexxus must pre-approve any inconsistent uses in writing.

Conexxus recognizes that a Member may wish to create a derivative work that comments on, or otherwise explains or assists in implementation, including citing or referring to the standard, specification, protocol, schema, or guideline, in whole or in part. The Member may do so, but may share such derivative work ONLY with another Conexxus Member who possesses appropriate document rights (i.e., Gold or Silver Members) or with a direct contractor who is responsible for implementing the standard for the Member. In so doing, a Conexxus Member should require its development partners to download Conexxus documents and schemas directly from the Conexxus website. A Conexxus Member may not furnish this document in any form, along with any derivative works, to non-members of Conexxus or to Conexxus Members who do not possess document rights (i.e., Bronze Members) or who are not direct contractors of the Member. A Member may demonstrate its Conexxus membership at a level that includes document rights by presenting an unexpired digitally signed Conexxus membership certificate.

This document may not be modified in any way, including removal of the copyright notice or references to Conexxus. However, a Member has the right to make draft changes to schema for trial use before submission to Conexxus for consideration to be included in the existing standard. Translations of this document into languages other than English shall continue to reflect the Conexxus copyright notice.

The limited permissions granted above are perpetual and will not be revoked by Conexxus, Inc. or its successors or assigns, except in the circumstance where an entity, who is no longer a member in good standing but who rightfully obtained Conexxus Standards as a former member, is acquired by a non-member entity. In such circumstances, Conexxus may revoke the grant of limited permissions or require the acquiring entity to establish rightful access to Conexxus Standards through membership.

Disclaimers

IF YOU ACQUIRE THIS DOCUMENT FROM CONEXXUS, THE FOLLOWING DISCALIMER STATEMENT APPLIES:

Conexxus makes no warranty, express or implied, about, nor does it assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any third party intellectual property rights (IPR) encumbrances, it cannot guarantee that such IPR does not exist now or in the future. Conexxus further notifies all users of this standard that their individual method of implementation may result in infringement of the IPR of others. Accordingly, all users are encouraged to carefully review their implementation of this standard and obtain appropriate licenses where needed.

Table of Contents

1 Introduction

This document is a guideline for implementing Open Retailing JSON messages using the RESTful web services transport mechanisms. This guideline helps to ensure that implementations can interoperate with minimal development and configuration.

1.1 Audience

The intended audiences of this document include, non-exhaustively:

- Architects and developers designing, developing, or documenting RESTful Web Services; and
- Standards architects and analysts developing specifications that make use of Open Retailing REST based APIs.

1.2 Background

RESTful web services have become popular in large part because the HTTPS infrastructure is so powerful and predictable. While there are certainly alternatives to HTTPS where speed of execution is a critical issue, the additional complexity of the alternatives, the increased difficulty of structuring tests reliably, and the ability to maintain the code are also important considerations.

This document focuses on how to use HTTPS transport for RESTful Web Services to the best advantage, since the advantages of using it, in terms of promoting interoperability, are quite substantial. Though concerns over the use of HTTPS in all cases are *not* completely unfounded, and other alternatives might be a bit “faster” in execution, those alternatives will undoubtedly suffer with impaired interoperability.

The RESTful web services world focuses on Web Servers and Clients. Denizens of this web services world have access to all of the following possibilities. These are listed in “simplicity first” order (see sections in 2.1 Standard HTTPS and OAS 3.0 Features for Performance below); consideration of an alternative for application implementation should always be in simplest first order.

In the paragraphs that follow is a summary of some of the key options available for tuning the HTTPS implementations.

Balancing performance requirements of the application with interoperability benefits should take priority when considering these options.

2 REST APIs Using HTTPS

Aspects to consider when using HTTPS as a transport for RESTful APIs include:

- HTTPS is half duplex;
- HTTPS is "Request – Response" – clients must "pull" data from the server, but the server can't "push" data to the client if server state changes. Client applications must poll the server for new information by repeating requests to see if there was any change of state on the server. In a "real-time" application, the required high frequency of polling may put a large load on both the client and the server;
- By default, HTTPS will open a new socket for each request. Well designed web server implementations have ways to mitigate this issue – see below; and
- Server state may dictate required subsequent client behavior – HTTPS is essentially a "stateless" protocol. Sometimes, a series of prescribed messages is required to lead the server through the required states, tightly binding the client logic to the server requirements.

The following section enumerates some key features that can help mitigate some of these potential issues.

2.1 Standard HTTPS and OAS 3.0 Features for Performance

2.1.1 HTTPS with Keep Alive

"Keep Alive" is a feature which allows server and client to maintain a persistent connection between calls, reducing call setup time (which includes TLS negotiation). See your server documentation for details.

Both client and server have to be ready to participate, but it can make communications much faster.

2.1.2 Links in Response Messages

OAS 3.0 supports the inclusion of "links" in response messages, giving the client instructions (i.e., "Hypermedia") on what comes next. Links may be described in the OAS 3.0 file or in the response body as described below under "HATEOAS".

"Links" are worthy of mention as the better way to solve some client/server interactions that otherwise might involve "call-backs." For instance, EPS uses a `DeviceRequest` message within the time frame of a `CardRequest` message. Using "links," the `CardRequest` would return an initial success response but with directions (links) describing what to do next, i.e., post the answer to a prompt (a `DeviceRequest` call-back in today's EPS). See "OAS 3.0 Links" in the References section contained in the Appendices.

HATEOAS (HAL) is closely related to "links," to RFC 5988, and to the Richardson Maturity Model for evaluating APIs. Using HATEOAS in a consistent way can handle many situations where the subsequent need for a server "call-back" is known when the server responds to an API call. For instance, the POS to EPS application protocol could easily use HATEOAS allowing each response message to inform the client what to do next (e.g., request next prompt.)

2.1.3 Server Sent Events

In HTML5, browsers (acting as clients) have a JavaScript API to open an event source on the server. The format of these events is standardized as two fields, "event:" and "data:"; the data can span many lines, and the event ends with an empty line (much like how HTTP indicates the end of headers and the beginning of message-body). Server sent events are a great way to enable, for example, chat-room software. They eliminate latency lags on the client. For relatively small messages, the event can contain required information, or the event can suggest that the client "pull" data with an API call.

2.1.4 Web Sockets (Secure Web Sockets)

Main considerations before implementing a Web Socket as part of an API include:

- Web Sockets are full duplex;
- Web Sockets are bi-directional;
- Service Push is core functionality of a Web Socket;
- Widely supported by web browsers and other client and server software stacks;
- Like Server Sent Events, the socket that is connected to the server stays "open" for communication. That means data can be "pushed" to the browser in real-time on demand;
- WebSocket is a low-level protocol, think of it as a socket on the web. Everything, including a simple request/response design pattern, how to create/update/delete resources, the meaning of status codes, etc. needs to be built on top of it. All of these features are already well defined for HTTPS;
- HTTPS supports a lot of other useful features such as data caching, intelligent routing, multiplexing, gzipping for large data, and lot more. All of these must be redefined on top of WebSocket; and
- The security infrastructure needs to be rebuilt from scratch.

When true high-speed or high-speed bi-directional communication is required, Web Sockets are always available, but they should be used only when necessary, like native C-code or assembly language.

2.1.5 OAS 3.0 (Swagger) Callbacks

OAS 3.0 has the ability to define "call-backs" within an API. While the OAS callbacks are defined in the language, implementing them requires an additional client-side API HTTPS Server end point. In the future, with a constellation of cloud-based services, the availability of an HTTPS Server for every API endpoint might be taken for granted. But at the current time, the other options serve the required use cases better.

2.2 HTTPS/2

The use of HTTPS/2 could help manage connections better because it decreases latency and improves response speed with additional features:

- Data compression of HTTP headers;
- HTTPS/2 Server Push;
- Pipelining of requests;
- Fixing the "head-of-line blocking problem" in HTTPS 1.x; and
- Multiplexing multiple requests over a single TCP connection.

Other advantages:

- It supports common existing use cases of HTTPS, such as desktop web browsers, mobile web browsers, web APIs, web servers at various scales, proxy servers, reverse proxy servers, firewalls, and content delivery networks; and
- It maintains high-level compatibility with HTTPS 1.1 (for example with methods, status codes, URIs, and most header fields). It creates a negotiation mechanism that allows clients and servers to elect to use HTTPS 1.1, 2.0, or potentially other non-HTTPS protocols.

3 Technical Aspects and Conclusion

3.1 Performance Comparison

Several studies have been done on performance, and certainly above 5000 requests per second, web sockets always win. Although again this depends on the environment and caching, etc. But in simple implementations, benchmark comparisons conclude that web sockets performance is better than standards HTTPS.

Nonetheless, while Web Sockets are "faster" than HTTPS, it's also true that machine language is faster than higher-level languages, like Java or C#. But use of machine language is not justifiable for a given implementation based only on the need for speed in some cases. The analogy holds between HTTPS and Web Sockets in the same way – HTTPS is the workhorse, with the emphasis on interoperability, while Web Sockets are available for 1) high speed / multi-message requirements and 2) for instances where asynchronous call-backs are required (though there are other ways to do that as described above).

The following statement extracted from the web says it all:

> *Web Sockets provide a richer protocol to perform bi-directional, full-duplex communication. Having a two-way channel is more attractive for things like games, messaging apps, collaboration tools, interactive experiences (inc. micro-interactions), and for cases where you need real-time updates in both directions.*

3.2 Security Considerations

Security is not a differentiator between alternatives for choice of transport. All have Secure implementations, i.e., HTTPS and WSS (Secure Web Sockets). In terms of authentication, no alternative appears to have material advantages over any other.

See "Open Retailing API Implementation Guide – Security" for more details

4 Conclusion

Based on the current level of research and discussion at the Joint API WG – which should continue – the conclusion is to support all transport options available for API based RESTful web services, with preference given to HTTPS. For some situations, there may be rare but insurmountable performance issues. In these situations, the lack of interoperability may outweigh the need for an alternative. But again, these situations will be rare.

In summary, all of the features described above **are** available for anyone implementing an API using a web server as an end point:

1. Plain HTTPS;
2. HTTPS with keep alive;
3. Links;
4. Server Sent Events [SSE];
5. Web Sockets; and
6. OAS Callbacks – heavy-weight truly bilateral server-to-server kinds of APIs.

These six alternatives are in increasing order of complexity. When a designer looks at the implementation requirements, the first one in the list able to meet them satisfactorily should be selected in order to maximize interoperability.

HTTPS/2 is a possibility for use in implementations, with a feature set orthogonal (i.e., separate and not replacing) to the alternatives above, and warrants further discussion.

5 Open Issues

- The tenets in section 3.2 Security Considerations to be confirmed by reference to the Security WG in IFSF and TAC in Conexxus.

6 Appendices

A. References

A.1 Normative References

IFSF Standard Forecourt Protocol Part II-3 IFSF Communications over HTTP Rest:
https://www.ifsf.org

IFSF Standard Part I-01 IFSF Glossary – Abbreviations, Mnemonics and Definitions:
https://www.ifsf.org

A.2 Non-Normative References

OAS 3.0 Links:
https://swagger.io/docs/specification/links/

HTTP/2:
https://en.wikipedia.org/wiki/HTTP/2

REST vs WebSocket Comparison and Benchmarks:
http://blog.arungupta.me/rest-vs-websocket-comparison-benchmarks/

B. Glossary

Term	Definition
API	**A**pplication **P**rogramming **I**nterface. An API is a set of routines, protocols, and tools for building software applications
Open Retailing	Open Retailing means both Service (Gas) Station and Convenience Store.
IFSF	**I**nternational **F**orecourt **S**tandards **F**orum
Internet	The name given to the interconnection of many isolated networks into a virtual single network.
JSON	**J**ava**S**cript **O**bject **N**otation; is an open standard format that uses human-readable text to transmit data objects consisting of properties (name-value pairs), objects (sets of properties, other objects, and arrays), and arrays (ordered collections of data, or objects. JSON is in a format which is both human-readable and machine-readable.
OAS	OAS (OpenAPI Specification) is a specification for machine-readable interface files for describing, producing, consuming, and visualizing RESTful web services. The current version of OAS (as of the date of this document) is 3.0.
Port	A logical address of a service/protocol that is available on a particular device.
REST	**RE**presentational **S**tate **T**ransfer) is an architectural style, and an approach to communications that is often used in the development of Web Services.
Service	A process that accepts connections from other processes, typically called client processes, either on the same device or a remote device.