RESO Web API Security - RESO Position . . . . . .

RESO Web API Security - RESO Position

1. Introduction

The goal of this paper is to define the scope of RETS Web API Security efforts. This paper relates to the initial implementation requirements, specifically related to the 1.0.1 standard definition. As the standard evolves and grows, additional papers may be written to encompass new thoughts around this topic.

This paper attempts to outline the following:

1. The objectives for the first standard release
2. What is in scope for the first release
3. What is not in scope for the first release
4. The rationale for the scope
5. How to influence the direction and scope going forward

This paper will not discuss the standard recommendations specifically, nor will implementation be covered. Those topics are fully detailed in the RETS Web API Security 1.0.1 standard document on the RESO Collaboration Portal.

2. Web API Security: Objectives

The initial objective for the Web API Security workgroup has been to define the best choice (or choices) to implement security in support of RESTful API development. Specifically, this initiative has been tied to the creation of a new RESTful API standard for providing access to real estate data.

Given this objective, this work does not (currently) attempt to define and recommend a standard for previous versions of RETS

3. Web API Security: Scope

Given the objective stated above, the scope of the initial standard work has been limited to fit the use cases and scope defined within the RESO Transport Workgroup and specifically the RETS Web API 1.0.1 standard.

The overall scope encompasses:

1. Read-only data access
2. Use within a RESTful architecture
3. Web, mobile and desktop interactive clients

Specifically, the security model supported in the first phase of the standard is the typical three-way authorization of a user (Transient authentication of an API Consumer on behalf of an MLS member). See Section 6.1.1 of the standard.

Example: A web application that interacts with the MLS on behalf of a user, e.g., a real-time CMA, and IDX website, mobile IDX search.

The specific use scenarios used as reference in defining the most appropriate standard are as follows:

Use Scenario 1 – A web application (e.g. a SaaS CMA application) accesses RESO Property records from an MLS Data Service on behalf of MLS Users so that users can build robust CMA reports.

Use Scenario 2 – A mobile application accesses RESO Property records from MLS Data Service on behalf of MLS Users so that users (e.g. real estate agents) may access data they have rights to see from their mobile device.

Comments Below
Use Scenario 3 – A listing syndication service provider accesses RESO Property records from MLS Data Service on behalf of End Users in order to syndicate MLS data to others.

Use Scenario 4 – A website provider accesses RESO Property records from MLS Data Service on behalf of MLS Users to create (IDX) websites where anonymous End Users (consumers) may view listings data.

These scenarios represent the most common read-only uses that the Web API standard focused on in its first release. These are direct MLS-User (e.g. member / agent) access or access on behalf of the MLS-User by a consumer/end-user.

4. Rationale

While there are many more use cases that could be supported by the standard, (and most certainly will over time) the initial goal has been to focus on incremental steps toward real-time data access. Specifically, the focus is currently on read-only access. As such, the Security Workgroup has tried to present what it believes is the best fit for the need.

We also believe the recommended approach does not limit use cases to those described above, it simply focuses, on ensuring those cases are well-supported.

5. Web API Security: Not In Scope

Not in scope for this initial rollout of the security standard are the following cases:

1. Server or Client to Server authorization (without human intervention) such as
    a. Database replication
    b. Database triggers
    c. Batch record updates
2. Transparent three-way authorization of a user. (Transient authentication of an API consumer on behalf of a user without human intervention)
3. Transparent, recurring ""on behalf of"" authorization of a user. (Persistent, transient authentication of an API consumer on behalf of a user without human intervention)

While many of these use cases “may” be supported by the proposed approach, this has not been the focus and therefore these have not been considered as part of the vetting process for the phase one standard.

6. Web API Security: Proposal

The proposed approach laid out within the following standard document utilizes an existing, widely-adopted standard that was designed to support the core use-cases described. The standard we will follow is the OAuth 2.0 RFC 6749 standard which has been developed and managed by the Internet Engineering Task Force (IETF).

We believe that OAuth 2.0 provides both a solid foundation for current needs plus the ability to support foreseen use cases beyond the current scope. We also know, however, it may not fit every use case or adequately address needs associated with all RESO standards. Therefore, additional security approaches may be added to the standard in support of those additional and alternative use cases.

7. Security Roadmap

The Security Workgroup will continue to collect use cases that go beyond this initial scope and encourages the community to help generate and solidify those use cases. To participate in that process you simply need to provide a brief description of the business requirement, a summary of the use case and, if available, a proposed approach to fulfilling the need.

Submissions may be made on the RESO Collaboration Portal in the Transport Discussions Section or they may be sent directly to Transport Workgroup Chair, Scott Petronis (spetronis@onboardinformatics.com) or Co-Chair, Matt McGuire (MpMcGuire@corelogic.com).