IPAWS Server2Server Bridge

KJ7BRE Communications - Updated: 06/22/21 - Version: 1.3 - ipaws@kj7bre.com

Evan Vander Stoep
Lead Developer/Manager
https://kj7bre.com
evan@kj7bre.com

The KJ7BRE Communications IPAWS Server2Server Bridge (S2SB) is a 3rd party data broker server for the Federal Emergency Agency Integrated Public Alert & Warning System (FEMA IPAWS) for use by hobbyists in the Emergency Alert System community. Data from FEMA IPAWS is retrieved at a fixed rate of every 30 seconds and is intended to be pulled by applications developed by individually approved hobbyist developers who have access to the S2SB.

The function of the S2SB is to give access to the public alert data without giving access to the FEMA issued pin for KJ7BRE Communications and to rate limit the total requests to the IPAWS servers. This is accomplished with a separate pin that is generated for use with the S2SB but does not give direct access to the IPAWS servers. It should be mutually understood among all developers who have gained access to the S2SB that their access is a privilege and not a right, meaning it can be revoked at any time without notice. Because of this, the S2SB should only be used by hobbyists and should never be used in a situation where the life, health or property of others is at risk.

Developers also agree to not pull from the S2SB at intervals less than 30 seconds. It should be noted that the reason for this is that the S2SB pulls alert data from FEMA IPAWS every 30 seconds, so if a developer connected to the S2SB was to pull at an internal rate less than 30 seconds, it would have no effect on receiving alerts faster as the S2SB is already rate limiting the requests to FEMA IPAWS.

Developers also agree to not share their pin with any other entity and if their pin is leaked, to notify KJ7BRE Communications (ipaws@kj7bre.com) in a timely manner. Developers should not be the ones to take action on the unauthorized person in which their pin has been leaked to. Once the issue has been resolved, a new pin will be generated for the developer and the previous pin will be disabled.

If any of these requirements are not met or there has been a previous history of a developer's actions that would raise concern, KJ7BRE Communications reserves the right to disable a developer's pin or deny an applicant to the S2SB at any time without prior notification.

Guidelines Overview

- Do not share pin with any other entities other then the original applicant
- If pin is leaked, notify KJ7BRE Communications (ipaws@kj7bre.com) in a timely manner.
- Pulling at intervals less than 30 seconds is prohibited
- Hobbyist use only (Non-Commercial Use)

Inorder to apply, developers must provide a valid email address and their intent in which they plan to use the S2SB. When submitting your application, you agree to all the rules outlined in this document.

For more information on how the Common Alerting Protocol is formatted and recommendations for best practices to follow, please refer to the documentation provided below (Courtesy of OASIS & ECIG).

OASIS Common Alerting Protocol Version 1.2 (oasis-open.org)
Integrated Public Alert and Warning System Profile Version 1.0 (oasis-open.org)
CAP to EAS Implementation Guide (EAS CAP Industry Group - ECIG

If you have any questions, comments or concerns about the Server2Server Bridge, please contact:

ipaws@kj7bre.com