Auddly IPN verification

Technical Interface Specification

Version: 1.0

Table of content

Introduction

The purpose with this document is to explain the International Performer Number (IPN) verification integration between a Collective Management Organisation (CMO) and Auddly.

This solution provides users the ability to verify their IPN without actually knowing the IPN number.

An Auddly user initiates the authentication process inside the Auddly web by selecting the CMO. User is then redirected to a login mechanism hosted by selected CMO. Could be a username / password login form, but this is up to the CMO to decide.

If the user is successfully authenticated the user is redirected back to Auddly. The return URL contains the selected (if several) IPN.

The IPN is now verified and can be used for registrations from Auddly.

Step 1: Auddly redirect user with return URL

The end user select action to verify their IPN with CMO inside the Auddly web platform.

Auddly generates a unique, temporary return URL which is valid for one hour. Generated return URL example:
https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy

Auddly generates a MAC of this URL as a whole (including protocol, domain, path and query parameters) using HMAC with a secret key shared with CMO. Example MAC created using openssl:
echo -n "https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy" | openssl dgst -sha256 -hmac "shared_key"
add170c420868151405aa9381c28236daa6681eb1fc026e4f9371a37919da671

User is redirected (https) to a login mechanism hosted by the selected CMO (could be a username/password login form). URL and MAC is attached to the CMO redirect as GET query parameters.

Complete CMO URL:

https://example.cmo.tld/?ret=https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy&mac=c2423c6ec2a46b9c76312febac024fa670b8da58a65a0644eeb4dd15c5916820

CMO validation check:
hmac(shared_key, url_param("ret")) = url_param("mac")

Step 2: CMO

User log in using their CMO credentials or another way to authenticate towards the CMO. The provided return URL is validated with the MAC. If the MAC doesn't validate the request should be considered harmful (not originated from Auddly).

To be decided by the CMO - if multiply IPN is registered on the user. Shall the user select the IPN to be used with Auddly or is there a default IPN.

The user is redirected back to Auddly. Selected IPN is added to the return URL provided by Auddly. A new MAC is created for the new return URL (Auddly provided URL + IPN query parameter) using HMAC with secret key. MAC is added to the return URL

Generated return URL example:
https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?ipn=123456789

Example MAC created using openssl:
echo -n "https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?ipn=123456789" |
openssl dgst -sha256 -hmac "shared_key"
9cac5709f0227acd1919b785c54e441e3ca25b28dc6717efb4d60b2759de2b42

Complete Auddly URL:
https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?ipn=123456789&mac=c9b1c678b2d99814e17daa3a7c85d53b4763204bd39d2cac758cc95a61cf73b7

User is redirected to this new URL. Return cases:

- IPN verification successful
- IPN error code

In case the IPN lookup fails the user should be redirected back to Auddly with an error query parameter. List of error codes:

Error code	Description
100	User requested return to Auddly: User did not try to authenticate but returned to Auddly using the “Return to Auddly” link
110	Authentication failed: User has failed authentication and returned to Auddly using the “Return to Auddly” link.
120	Invalid Performer: User is successfully authenticated but not identified as a performer.
130	IPN Missing: User is successfully authenticated and identified as a performer but CMO do not have an IPN.

Generated return URL example:
https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?err=120

Example MAC created using openssl:
echo -n "https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?err=120" | openssl dgst -sha256 -hmac "shared_key"
1f9d554cb8adbbeb95d601b28129b22108ffebfff3d776f838f4dde44bf64ac6

Complete Auddly URL:
https://app.auddly.com/1o4or8xn8h14ve85kob12i745mpklfoy?err=120&mac=1f9d554cb8adbbeb95d601b28129b22108ffebfff3d776f838f4dde44bf64ac6

Step 3: Auddly validates URL

Auddly receives the user on the unique, temporary URL.
Auddly creates a MAC of the whole URL and verifies that it matches the provided MAC.
Auddly ensures that its the same user “coming back” as the one whom the temporary URL was created for.
The user is then IPN verified with the IPN provided in the URL.

Auddly validation check:
hmac(shared_key, url_without_mac) = url_param(“mac”)

Security

All communication is done over SSL/TLS.

The temporary URL generated by Auddly has a TTL of 1 hour.
MAC function used is HMAC-SHA256 and the MAC is hex encoded in the URL.
A routine for rotating shared secret keys should be in place.

Appendix - Document control

Change history

Version	Date	Author	Comments
0.1	01/09/15	Fredrik Simón	First version
0.2	22/09/15	Emil Wallinder	Added redirect cases
0.3	23/09/15	Fredrik Simón	Added error handling
1.0	25/09/15	Emil Wallinder	Document reviewed