Ad-ID COMPLETE EXTERNAL ACCESS (CEA) SPECIFICATION

Version 1.3

Revision History

Date	Updates
April 2016	Version 1.3 – Added description/example of default Industry Group
November 2015	Version 1.2 – Included Authentication/Request specification for CEA service
July 2015	Version 1.1 – External Specification
January 2014	Initial Specification 1.0

GOAL

Ad-ID Complete external access (CEA) is a tool to provide basic existence validation and slate information for pre-known Ad-ID codes to a select group of registered users through an API-only interface.

Media outlets will be guaranteed access to CEA, this includes online publishers. Measurement companies and other companies will need to request access via CEA, and granted by a process that is yet to be determined. Companies that do not qualify for CEA, will need to use Ad-ID's Selective External Access (SEA). For details on SEA refer to http://ad-id.org/about/external-access.

CEA does not provide any directory (lookup) or search services. Users of CEA must know what they are seeking.

CEA is a read-only service and will not modify Ad-ID's in any manner or form.

USERS

Users of Complete External Access (CEA) must request access through customer service and be approved. This request should include basic information about the CEA account including, but not limited to, contact name, email, address, etc. For the approval process, users may be required to submit a "purpose of use" statement, which will be evaluated before granting access. Users also must accept the terms of service for CEA.

Upon approval of the account, Ad-ID will issue a CEA USER ID and CEA API KEY. All CEA calls must contain both keys as part of the request to gain access.

The purpose of the CEA USER ID and API KEY is to bind the user and their use of the service to the terms and conditions for the service. Requests containing a user's CEA USER ID and KEY are the responsibility of that user – thus requiring them to guard these keys in an appropriate manner.

AD-IDS

Ad-ID records will be marked with a flag (cea_flag) indicating the access status to CEA service. CEA_flag will be available in the UI and provide users the ability to toggle if a record is made available for CEA or not.

The two possible states controlled by CEA flag (cea_flag) are:

1. Allowed – select information will be made available about the particular Ad-ID via CEA (Default)
2. Denied – (under limited conditions) no detailed information will be made available about the particular Ad-ID via CEA, other than that it is a valid Ad-ID and the Parent company (if available).
    - Parent company will not be available for Ad-ID whose prefix is not associated with a corporate parent (“unlocked”)

The default will be to allow access (Allowed) to Ad-ID data.

Note: CEA_flag is not part of the response returned from CEA service and only used to determine if a record is available or not as part of CEA.

CEA PROTOCOL

There are no authentication requirements for CEA beyond CEA KEY and signed request. CEA service is separate and apart from the core users of the Ad-ID web-based system. No web system credentials should ever be solicited or passed to CEA gateway.

There is only a single CEA request defined for version 1 of this product. It is designed to return information on a single Ad-ID. Future versions may permit multiple Ad-ID's per request, but this is not part of Phase 1.

CEA request is a standard HTTPS RESTful request.

The request will contain the following headers:

1. x-userid (CEA user id provided by Ad-ID)
2. x-date (an ISO 8601 format date/time of the request)
3. x-hash (a hashed value of the url and the date/time per Ad-ID specifications).

The request will contain the following parameters:

1. The complete Ad-ID being requested (key=CODE)
   OR
2. The compact unique identifier (cuid) for an Ad-ID being requested (key=CUID)

Example Request:
cea.ad-id.org/adid_services/ea_c/adid/ADID0001000
or cea.ad-id.org/adid_services/ea_c/cuid/abf6cda3

There are three possible response codes for any given CEA REQUEST. They are:

1. Code=0 : The Ad-ID was found and the information is contained in the balance of the response
2. Code=1 : The Ad-ID does not exist
3. Code=2 : The Ad-ID is valid but the information requested is denied as described above

The entire response will be a well-formed XML document similar to the following:

```
<response>
        <status> [status code from above] </status>
        <count> [the number of codes returned in this query, set to 1 or 0 for V1] </count>
        <status_message>[Status Message] </status_message>
        <codes>
                <code>
                        <adid> [the adid code] </adid>
                        <guid> [the adid compact identifier ] </guid>
                        <field 1> … </field 1>
                        <field n> … </field n>
                </code>
        </codes>
</response>
```

All valid requests will return an HTTP 200 response.

Invalid CEA KEYS or a bad signature request will generate an HTTP 403 response code.

Poorly formed requests will generate an HTTP 4xx code.

Ad-ID DIGITAL AD SLATE AND ADDITIONAL METADATA

CEA service will return an XML document containing Ad-ID Digital Slate, Product Categorization and Commercial Delivery Companies from External Access that are selected for that code. See Appendix A for an example.

APPLICATION LOGIC

When a CEA request enters the gateway, the following is a high level workflow; each generating an appropriate response

1. Is the request well-formed?
2. Does CEA KEY exist and is it valid?
3. Is the user authorized to access CEA:
    a. Is CEA KEY/Signature permitted and valid?
4. Does the requested Ad-ID exist in the Ad-ID system?
    a. If the Ad-ID does not exist at all; return status 1
    b. Is the code “voided”? -> return status 2
    c. Is CEA_flag on the record set to “deny”? -> return status 2
    d. Is CEA_flag on the record set to “allow”? -> return status 0
5. Log request
6. Deliver response

Sample responses are in Appendix A and B.

METADATA UPDATES AND CHANGES

Any changes to the metadata will be applied and will be up-to-date, but providing the ability to receive notification for these updates is beyond scope for the initial phase.

CEA SERVICE – AUTHENTICATION AND REQUESTS

CEA Authentication

CEA Authentication is a process by which the identity of the request to CEA server is verified. All HTTP traffic for CEA will take place over SSL and use a pure form of the RESTful API. CEA authentication and requests will require the generation of a HMAC signature along with one additional value (date/time). The Date/Time should be in ISO 8601 (RFC3339) format.

Overview of the authentication process

1. A user obtains a CEA User ID and CEA API Key.
2. The user submits a request with the credentials to CEA server.
3. CEA server uses the credentials to verify the request is from a valid CEA user.
4. If the credentials are valid, the request is processed, and response information is returned. If the credentials are invalid, the recipient rejects the request and returns an error message.

CEA Credentials

Each CEA account must be provisioned with the following elements:

1. CEA User ID – (a 8-character, alphanumeric sequence)

   Example:
   CEA User ID: A8U978X0

2. API Key – (a 16-character, alphanumeric sequence)

   Example:
   CEA APIKEY: A8U978x0b9K123X9

CEA Requests

All requests to CEA server will be made over SSL with the following headers (sha256 used in this example):

GET /adid_services/ea_c/adid/ADID0001000

X-Userid: A8U978X0
X-Date: 2015-10-08T10:00:00-04:00
X-Hash: 7cc4d54522a2b45835c14b4fa87a7e7adaaa503452ab38443e3bf55eb0d94a70

URI Format:

Only two URIs are supported by CEA as follows:

Method: GET

URI: /adid_services/ea_c/adid/ADID0001000
URI: /adid_services/ea_c/cuid/abf6cda3

HMAC-SHA256 Generation for REST Requests

Generation of the HMAC is based on the URI being requested along with one additional value: The date/time. The Date/Time should be in ISO 8601 (RFC3339) format.

Basic Authentication Process

The following describes the steps required to authenticate requests to CEA using an HMAC-SHA256 request signature.

1. You construct a request to CEA.
2. You calculate an x-hash message authentication code (HMAC-SHA256) signature with your CEA API Key. For information about HMAC, see RFC2104.
3. You include the following x-header info in the request, and then send the request to CEA.
    1. x-userid (CEA user id provided by Ad-ID)
    2. x-date (an ISO 8601 format date/time of the request)
    3. x-hash (a hashed value of the uri and the date/time per Ad-ID specifications).
4. CEA uses your user ID to look up your CEA API key.
5. CEA generates a signature from the request data and CEA key with the same algorithm you used to calculate the signature you sent in the request.
6. If the signature generated by CEA matches the one you sent in the request, the request is considered authentic. If the comparison fails, the request is discarded, and CEA returns an error response.

APPENDIX A: INFORMATIVE EXAMPLE FOR RESPONSE cea_flag VALUE 0

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
      <status>0</status>
      <count>1</count>
      <adid>
       <adid_fullcode>ZADE0001000H</adid_fullcode>
       <guid>fb1a1dfe</guid>
       <slate>
          <media_type>Video</media_type>
          <video_format_flag>H</video_format_flag>
          <parent id="U10000160">AD EYE DEE CORP</parent>
          <advertiser id="C10000161">AD EYE DEE STORES</advertiser>
          <brand id="B10000162">EYEGLASSES</brand>
          <product id="P10000165">REGULAR VISION</product>
          <ad_title>Seeing is Believing</ad_title>
          <created>2015-09-25</created>
          <copyright>2015 Ad Eye Dee Corp</copyright>
          <version>Free case</version>
          <agency_name>Ad-ID, LLC</agency_name>
          <language>English</language>
          <length>30</length>
          <bleed></bleed>
          <color_type></color_type>
          <expandable></expandable>
        </slate>
       <Brand_and_Product>
          <industry_group id="G700">RETAIL</industry_group>
          <major_category id="G710">RETAIL STORES</major_category>
          <sub_category id="G71E">OPTICAL GOODS AND SERVICES</sub_category>
          <product_category id="G71E">OPTICAL CTR</product_category>
       </Brand_and_Product>
       <commercial_delivery>
          <group>Extreme Reach</group>
        </commercial_delivery>
    </adid>
</adids>
```

Access Allowed for an Ad-ID that includes a specific product.

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
      <status>0</status>
      <count>1</count>
      <adid>
       <adid_fullcode>ZADL0002000H</adid_fullcode>
       <guid>8448b0f7</guid>
       <slate>
          <media_type>Video</media_type>
          <video_format_flag>H</video_format_flag>
          <parent id="U10000160">AD EYE DEE CORP</parent>
          <advertiser id="C10000161">AD EYE DEE STORES</advertiser>
          <brand id="B10000162">EYEGLASSES</brand>
          <product id="OTHER">Eye Care</product>
          <ad_title>See the Light</ad_title>
          <created>2016-04-12</created>
          <copyright>2016 Ad Eye Dee Corp</copyright>
          <version>Spring Special</version>
          <agency_name>Ad-ID, LLC</agency_name>
          <language>English</language>
          <length>60</length>
          <bleed></bleed>
          <color_type></color_type>
          <expandable></expandable>
        </slate>
       <Brand_and_Product>
          <industry_group id="G700" default=”true”>RETAIL</industry_group>
          <major_category></major_category>
          <sub_category></sub_category>
          <product_category></product_category>
       </Brand_and_Product>
       <commercial_delivery>
          <group>Extreme Reach</group>
        </commercial_delivery>
    </adid>
</adids>
```

Access Allowed for an Ad-ID that includes a product the user identified as “Other” and entered manually.

APPENDIX B: INFORMATIVE EXAMPLE FOR RESPONSE cea_flag VALUE 1

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
   <status>1</status>
 <status_message> The Ad-ID was not found</status_message>
  <count>0</count>
</adids>
```

APPENDIX C: INFORMATIVE EXAMPLES FOR RESPONSE cea_flag VALUE 2

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
   <status>2</status>
  <status_message>The Ad-ID is valid but has been excluded.</status_message>
   <count>1</count>
   <adid>
      <adid_fullcode>ZADL0001000</adid_fullcode>
      <guid>ff8ec4bf</guid>
      <parent>XYZ Corporation</parent>
   </adid>
</adids>
```

Access Denied for Ad-ID whose prefix is associated with a corporate parent ("locked").

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
   <status>2</status>
  <status_message>The Ad-ID is valid but has been excluded. Parent company information is not
available.</status_message>
   <count>1</count>
   <adid>
      <adid_fullcode>ZADL0001000</adid_fullcode>
      <guid>ff8ec4bf</guid>
   </adid>
</adids>
```

Access Denied for Ad-ID whose prefix is not associated with a corporate parent ("unlocked").

```
<?xml version="1.0" encoding="UTF-8"?>
<adids>
   <status>2</status>
  <status_message>The Ad-ID has been voided.</status_message>
   <count>1</count>
   <adid>
      <adid_fullcode>ZADE0001000H</adid_fullcode>
      <guid>fb1a1dfe</guid>
   </adid>
</adids>
```

Voided Code – A user removed this code from the list of active Ad-ID codes.

APPENDIX C: Ad-ID CEA FIELD DESCRIPTIONS

Field Name	Required	Description
Full Ad-ID code	Yes	The unique identifier for this advertising asset. Includes Flag for HD or 3D.
GUID	Yes	Ad-ID Internal CUID (Compact Unique Identifier).
Media Type	Yes	The media category describing the type of advertising asset. Only one media type can be chosen per advertising asset Example: Video would be used for TV ads
Video Format Flag	Yes	Only available for codes with media type Video. Refers to SD (standard definition), HD (high definition) and 3D (3 dimensional).
Parent	Yes	The parent company of the advertiser featured in the advertising asset. Example: AD EYE DEE CORP
Advertiser	Yes	The company or the agency's client that is advertising. Example: AD EYE DEE STORES
Brand	Yes	The advertiser brand that is associated to this product. Example: EYEGLASSES
Product	Yes	The product that is the extension of the brand. Example: REGULAR VISION
Ad Title	Yes	Indicates the name of the advertising asset.
Length/Size	Yes	Indicates the duration or size of the advertising asset.
Agency Name	Yes	The agency working with the advertiser.
Language	Yes	The spoken language of the advertisement formatted according to the English Name Of Language of a registered RFC-5646 region code from ISO 639-2.
Copyright	No	Copyright information related to or communicated in this advertising asset.
Version	No	Describes a variation which differentiates this advertising asset from another. Example: A company runs the same advertising asset in 3 cities, but each one has a customized offer at the end for the specific location. All 3 advertising assets may have the same Ad Title, but the version indicates the city and/or the special offer included in the advertising asset to differentiate the 3 versions from each other.
Bleed	No	Only available for codes with media type Print. Indicates whether the print asset is a bleed or non-bleed ad. Bleed means the item runs up to the edge of the page.
Color Type	No	Only available for codes with media type Print. Indicates the color used in the print ad (Black and White, Four Color, etc).
Expandable	No	Only available for codes with media type Internet Display or Mobile. Indicates whether the ad is expandable or not.

Field Name	Required	Description
		Expandable means the ad expands in size when a user rolls over or clicks on them.
Date Created	Yes	Date the Ad-ID code was created.
Industry Group	Derived*	Most generic grouping, represented by a hundred level numeric code. Example: G700- RETAIL
Major Category	Derived*	Further refines the industry category, represented by a ten level numeric code. Example: G710- RETAIL STORES
Sub Category	Derived*	Most specific PCC level associated with brands, and represented by the unit level numeric code. Example: G71E- OPTICAL GOODS AND SERVICES
Product Category	Derived*	The most granular level used to identify the specific categories included in the PCC Sub Category. Example: G71E - OPTICAL CTR
Commercial Delivery	No	Companies that distribute ads to media outlets on behalf of advertisers and their agencies.

*These values are derived from the Product selected on the slate. If the value of "Other" is chosen, the user manually enters a product, in which case a default Industry Group will be provided and the other categories will not be populated.

APPENDIX D: Error Code Reference

The following is a reference guide for error codes and messages returned from CEA Web Services on validation errors or issues with our services.

- Authentication: bad credentials, userid/apikey mismatch, request received outside time limit based on timestamp in message. After X failures in X minutes system will begin to block by IP address and email tech.
- Malformed request - treated the same as authentication failure
- Request for nonexistent resource (adid or cuid not found). After X failures in X minutes, block by IP address for 30 minutes, no email notification to tech.

Error on Validation

Error Code	System Name	Description
1001	CEA_ERR_DATA	There is an error in one or more input data parameters in the request. Malformed Request
2001	CEA_ERR_AUTH	There is an error in CEA credentials provided in the request or the signed request is not valid.
5001	CEA_ERR_PROC	A processing error occurred.

System Response

HTTP Response Code	HTTP Reponses Text	Ad-ID Web Services Usage
200	OK	Success.
400	Bad request	Errors in input data parameters.
403	Forbidden.	Authentication errors, or attempting to access data for which the user is not authorized.
405	Method not allowed.	Attempting to pass request parameters using an unsupported http method.
500	Internal server error.	An error not covered by the other response codes.

Sample Response – XML

```
<?xml version="1.0"?>
<error>
</error_message>
 <error_code>2001</error_code>
 <error_message>Request data failed validation. Please address the issues and try
again.</error_message>
</error>
```