JSON Web Token Single-Sign-On Integration

Table of Contents

Overview

The majority of Rievent customers prefer to utilize a **Single-Sign-On (SSO)** authentication solution that enables a learner to navigate between the primary customer website and the Rievent Learning Portal without having to sign-in more than once. Rievent supports a standard **JSON Web Token Trusted Handoff Protocol** for SSO that is secure and easy to setup. It utilizes SSL and digital signature verification to enable customers to authorize authenticated users to access the Rievent platform and to transfer profile information and entitlements to restricted resources.

JSON Web Tokens

A **JSON Web Token (JWT or token)** is a compact format for transmitting data over the internet. A JWT consists of Base64-URL-encoded JSON representing a header and payload. A JWT header describes the properties of the JWT, such as information on the cryptographic algorithms applied. A JWT payload consists of one or more claims representing name-value pairs of the data being transmitted. These claims comprise the data necessary to complete a valid trusted handoff. To secure the contents of a JWT, the JWT can be digitally signed; for the Rievent Trusted Handoff Protocol, **all JWTs must be signed** to be able to verify the contents of the JWT and authenticate the learner into the Rievent Platform.

JSON Web Tokens can also be encrypted to further protect its contents. For the Rievent Trusted Handoff Protocol, **the payload of an encrypted JWT must be a signed JWT** containing all the claims necessary for a valid trusted handoff. For cases where the trusted handoff token could potentially be accessed and viewed by a third party (RieventConnect page embed script or HTTP GET request), Rievent encourages encryption of the overall token to provide better transport security and ensure the privacy of its contents.

JSON Web Signature (JWS)

A signed JWT (JSON Web Signature or JWS) is composed of three Base64-URL-encoded period (.) delimited fields:

- the JSON header
- the JSON payload containing learner claims and profile data
- the cryptographic signature of the Base64-URL-encoded, period-delimited, header and payload

JSON Web Encryption (JWE)

An encrypted JWT (JSON Web Encryption or JWE) is composed of five Base64-URL-encoded period (.) delimited fields:

- the JSON header
- the encrypted payload (typically symmetric) encryption key
- an initialization vector
- the encrypted payload containing learner claims and profile data
- an authentication tag

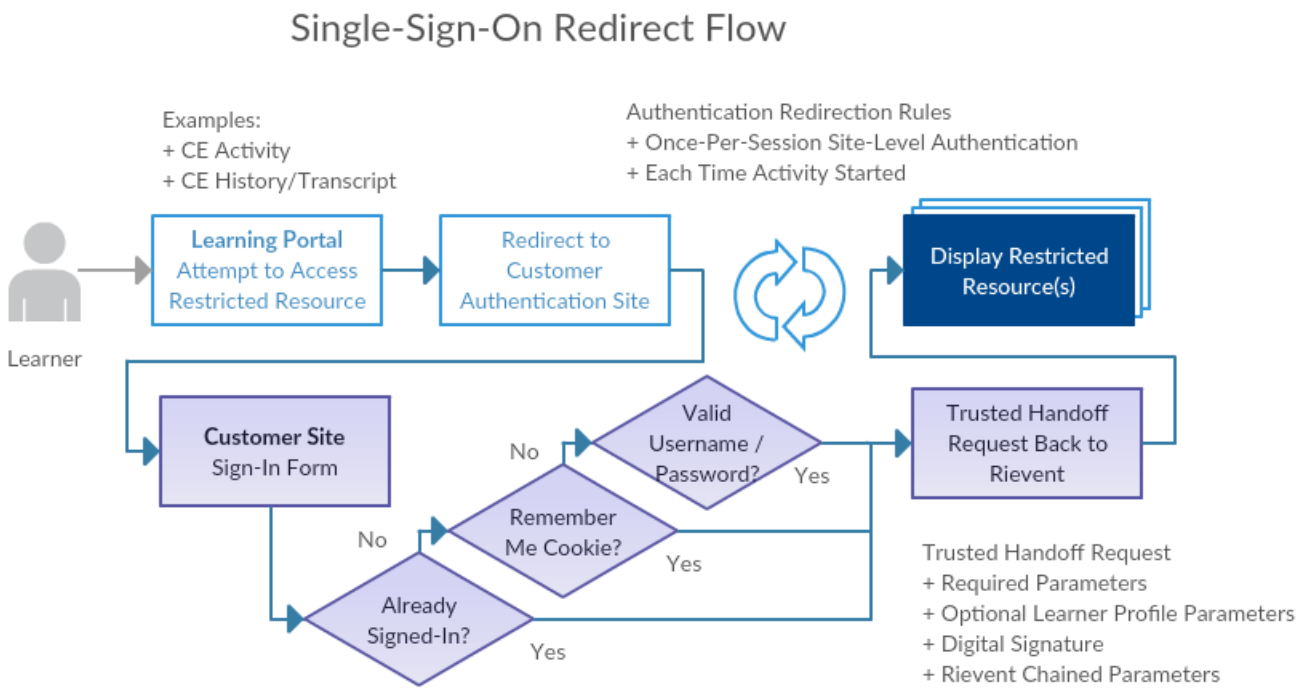
Additional Resources

For more information on JSON Web Tokens, including examples and library implementations for a variety of languages and environments, please see **JSON Web Tokens - jwt.io (https://jwt.io/)**.

Rievent Trusted Handoff Protocol

The **JSON Web Token Trusted Handoff Protocol** represents **the standard SSO solution** for the Rievent Platform. Integration partners are provided documentation instructing them how to construct and sign handoff requests to Rievent. The customer's Learning Portal in Rievent and all continuing education activities are pre-configured to accept trusted handoff requests. No additional custom development by Rievent is necessary in order for customers to utilize the Rievent standard SSO solution.

Rievent configures all entry points to restricted resources in the learning portal to redirect to the external customer authentication site and perform the authorization request. The customer is responsible for verifying the authenticity of the learner, determining their entitlement status for the requested resources, and then completing a trusted handoff request back to Rievent.



1. Learner attempts to access restricted resource.
2. Rievent redirects the learner to the customer authentication site, passing along a number of parameters that will be used by customer to create the trusted handoff request.
3. Customer authenticates learner via existing login session, "Remember Me" cookie, username and password, or other applicable means.
4. Customer compiles all **required parameter names and values** and, optionally, learner profile and entitlement information as claims for the trusted handoff token.
5. Customer appends all parameter name and values sent by Rievent during redirect request into the trusted handoff claims. (**Important**)
6. Customer creates a signed JSON web token using their RSA private key and all compiled claims. Rievent also encourages encrypting the token as a JWE.
7. Customer issues an HTTPS GET or POST request back to the appropriate site or activity level URL endpoint.
8. Rievent decrypts (where applicable) and verifies the signed JSON web token provided in the trusted handoff request using the RSA public key and enables learner access to the restricted resource.

Customer Setup Process

A number of setup steps are necessary before a customer can begin transmitting trusted handoff requests to their learning portal and educational activities.

1. Customer informs Rievent of desire to add a new external site "referrer" that will perform authentication and authorization requests to Rievent.
2. Rievent configures new "external referrer" record in the Rievent Platform and provides customer with the referrerId.
3. Rievent coordinates with the customer on generation and distribution of RSA keypair, used to digitally sign and verify trusted handoff requests.
    1. Rievent requires public key to be provided in either PKCS#8 (PEM-formatted) or Rievent proprietary format.
    2. Customer can generate keypair through Rievent Keypair Generator Tool: https://platform.rievent.com/tools/keypair.jsp
4. Customer develops digital signing code per the specification and unit testing against examples found on the Keypair Generator Tool.
5. Customer provides Rievent with the URLs of their authentication sites for QA and production.
6. Rievent configures QA environment for testing trusted handoff.
7. Integration testing site and activity-level trusted handoff in QA environment.
8. Customer provides acceptance and approval to go live.
9. Rievent configures Production environment for trusted handoff.
10. Integration testing site and activity-level trusted handoff in Production environment.

Obtaining the RSA Keypair

The trusted handoff request is signed and verified using an RSA private and public key pair. The keypair can be created using any number of widely available tools. The keypair must be provided in PKCS#8 (PEM) format, and the key size must be at least 2048 bits. Typically the customer should only provide Rievent with the public key as the private key is not necessary for validating the signed authorization token. It is not uncommon, however, during the testing phase of the SSO integration process, that Rievent be provided both the private and public keys so that Rievent can provide troubleshooting assistance, signing and comparing handoff requests against those issued by the customer. This can greatly accelerate the troubleshooting process during the integration testing phase. Once all issues are resolved, the customer can create a new keypair, providing Rievent only the public key component.

Keypair Generator Tool (https://platform.rievent.com/tools/keypair.jsp)

Rievent provides a utility page for generating 2048-bit RSA keypairs. The customer may use this page to obtain an RSA keypair in multiple formats, including PKCS#8. Additionally, the web page provides examples for common patterns of signing tokens to the trusted handoff service. Developers may use this information during unit testing their trusted handoff code to verify the tokens they are creating are consistent with the values expected by Rievent.

Working with Rievent Trusted Handoff

Rievent Redirect

The redirect request will contain a number of additional parameters and values that may be utilized by the authentication provider (where applicable) but are primarily provided for the purpose of being appended to the trusted handoff request back to Rievent. These parameters are required components of successful trusted

handoff resolution once the learner is returned to Rievent. They must be included, without modification, as claims in the trusted handoff token sent back to Rievent.

The number and type of parameters provided in the SSO redirect from Rievent may vary over time or differ based on the learning activity and unique requirements of the customer. A partial list of parameters that are currently commonly sent are described below, however other parameters may be sent. **The customer should always chain any redirect parameters back to Rievent as claims within trusted handoff token**. It is also possible for Rievent to include additional parameters as part of the SSO redirect that may be utilized by the authentication provider for determining finer grained learner access control and/or entitlements. Customers should inquire if there is a need for additional information to be sent by Rievent as part of the redirect for authentication.

Name	Description
`handoffUrl`	Identifies the appropriate endpoint to complete the trusted handoff of the authenticated learner back into the Rievent Platform.
`externalActivityId`	Unique identifier of the learning activity **within the customer system** and may be utilized for the purpose of determining per-activity entitlement statuses.
`accessCode`	Secondary unique alphanumeric identifier for the learning activity **within Rievent**.
`workflowMode`	Indicates the workflow of the learning activity, for example: registration, credit request, outcomes.

Creating a Trusted Handoff JSON Web Token

Overview

To create a signed JSON Web Token for a trusted handoff, you must first generate a name-value map of all of your trusted handoff claims. The list of required and optional trusted handoff claims are provided below. Once you have your claims, create the digital signature for your payload contents, and package all of the token contents as a Base64-URL-encoded, period-delimited, string. Rievent encourages using a JWT software library for creating and packaging your tokens. A wide range of libraries can be found for all major computing languages.

On signing your token, you will use your public key and should be sure to include your `referrerId` as the signature key ID in the JWT's header (as `kid`). Rievent currently recommends RSA256 with SHA2 signatures, which should be widely supported by a variety of JWT libraries. Your JWT library should set the appropriate signature algorithm header as needed ("alg":"RS256"). To complete the trusted handoff request back to Rievent, you will provide your signed JWT in the **`riejwt`** request parameter.

Example JSON Web Signature Header

```
{
        "alg":"RS256",
        "kid":"99"
}
```

Example Activity-Based Trusted Handoff Claims

```
{
        "exp":1589916451,
        "email":"learner@example.com",
        "accessCode":"ABCDEF",
        "externalId":"XYZ4321",
        "referrerId":"99"
}
```

Signing your JWT secures the handoff from being modified by any other party before it reaches Rievent; additionally encrypting your JWT will prevent its contents from being read by any other party outside of Rievent. If you opt to encrypt your signed JWT before handing it back to Rievent, you may use Rievent's public key for encryption (see below). When encrypting a JWT, be sure to set the identify of the Rievent encryption key through the key ID header on your encrypted JWT (JWE) to "1" ("kid": "1"). See you library's documentation for relevant information regarding selecting an encryption and key management algorithm. Rievent currently recommends RSAES with OAEP 256 key management ("alg":"RSA-OAEP-256") and AES-CBC128 with HMAC-SHA256 ("enc":"A128CBC-HS256"). Your library should automatically determine your initialization vector and authentication tag during encryption. The payload of your encrypted JWT must be your signed JWT - do not provide handoff claims directly within the payload. When providing a nested, signed, JWT as the payload of an encrypted JWT, you should set the content type header as "JWT" ("cty":"JWT"). Finally, using your library, serialize and base-64 encode the token and provide as the **`rietwt`** parameter in the trusted handoff request back to the Rievent **`handoffUrl`** endpoint.

Example Activity-Based Trusted Handoff Claims

```
{
        "cty":"JWT",
        "alg":"RSA-OAEP-256",
        "enc":"A128CBC-HS256",
        "kid":"1"
}
```

Rievent Encryption Public Key

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAkkAce9wk0HyPCjHjrKta
mPcfjkiJlfK+pcIIE2bGflIE3ZUNpYniGxLyynwS0FFmU4v5r49RDi3TqIvCFPF2
ke5EBYgyQ347iXl0heKWct7WYkGjcM23tLdRwF0yTGieLIFKf/A+l4PZf3E8qscN
za0tYC3H5NVfNJvuRZo1gkm4xv+giczYZfiA2WUr+X/S2WVse/TTWIUAb4T+dIhH
2FLWVD7F9z3V7luQ5QrytodsrNsUrNMwI2szZsA0Xz7hoxebXisf5KC/DFAzTOK+
0abgRPOkcqrx9+hsKPFD8mhLCDFqFCgiAEUuUoEYacVTuy3j4wGxa/CGUcFy+1uo
/wIDAQAB
-----END PUBLIC KEY-----
```

Trusted Handoff Endpoints

During the trusted handoff redirect from Rievent, the `handoffUrl` parameter will indicate where the trusted handoff should be completed following successful authentication. This is the endpoint that should be used to provide the trusted handoff token. The trusted handoff endpoint provided in the handoffUrl parameter may include one or more optional query parameters. If provided, these query parameters may contain important activity, or use case, specific re-initialization parameters. You should always use the handoffUrl as provided for the trusted handoff endpoint. For verification purposes only, the possible endpoints provided by the handoffUrl parameter are listed below. If you choose to verify the handoffUrl against the list below, allow for variations in the query string.

Destination	URL	Successful Result
Course History	https://<cme site domain>/s/signon/handoff	The personalized course history for the authenticated learner, indicating any in-progress or completed activities.
Course Catalog	https://<cme site domain>/s/catalog/handoff	The personalized course catalog for the authenticated learner, showing all published activities and indicating the learner's current progress in these activities, as appropriate.
Activity	https://<cme site domain>/attendee/view_program.jsp	The intended educational activity will be presented to the authenticated learner, bypassing any front matter. The learner may be prompted by a profile form if the activity is configured to require profile attributes that were not provided previously by the learner, or through the trusted handoff.

In the case of an **invalid trusted handoff** request, the learner will be presented a support page displaying the heading "An unexpected error has occurred...". You may contact Rievent technical support to assist with troubleshooting and resolving unexpected trusted handoff errors. It may be necessary to share your private key (or temporary keypair) to assist in the resolution process. You will be able to generate a new keypair (and provide Rievent the updated public key) once trusted handoff has proven successful.

Request Parameters

These following request parameters should be provided with the overall trusted handoff request back to the Rievent Platform. They should not be provided as claims within the JWT.

Name	Description	Data Type
`riejwt`	The base64-encoded JSON Web Token to complete the trusted handoff and authenticate the learner into the Rievent Platform.	TEXT
`mct`	**Optional.** The recruitment campaign tracker, provided to the customer on an as-needed basis.	NUMERIC

Required Claims

The following list of claims are the minimum required to complete a successful handoff request. They must be provided as the payload of the signed JWT. It is the responsibility of the authentication provider to correctly pass these claims. If any of these claims are missing or invalid, the handoff will fail and the learner will immediately be presented with a support request page.

All Handoffs

Name	Description	Data Type	Size Limit
`email`	The email address of the user being handed off. Must be unique within customer database.	TEXT	128
`referrerId`	The ID assigned to the external client. This is a static value provided to the customer by Rievent and should not change.	NUMERIC	
`externalId`	The unique learner ID in the customer system.	TEXT	64
`exp`	A timestamp (time in milliseconds since the Unix epoch) identifying the expiration time on or after which the JWT must not be accepted for processing.	NUMERIC	

Activity-Based Handoff

The following parameters must be additionally provided for handing off to a Rievent learning activity in order to identify and initialize or resume activity participation.

Name	Description	Data Type	Size Limit
`accessCode`	Unique course identifier. Generally this is **chained to the customer during course redirection from Rievent** for SSO authentication.	TEXT	64

Optional Profile and Other Claims

The following set of profile attribute claims are optional. It is up to the customer to identify which attributes exist in their existing system of record and determine which should be communicated as part of the trusted handoff request. Rievent recommends passing as much profile information about the learner that is available in order to bypass the profile form in the activity workflow and satisfy the requirements of a credit claim, populating a certificate, and reporting with accrediting bodies. The learner should expect to be prompted by a profile form if the activity is configured to require profile attributes that were not provided either by the trusted handoff, or by the the learner through the profile form in a previously attended activity.

Name	Description	Data Type	Size Limit	Notes
`entitled`	The learner's current entitlement status to the restricted resource (activity).	BOOLEAN		This parameter should only be passed when dealing with restricted content and/or eCommerce, in such cases where the Rievent Platform requires

Name	Description	Data Type	Size Limit	Notes
				awareness to show or bypass a paywall (or redirection to partner site).
prefix	Learner's prefix (Mr./Mrs./Ms./Dr.)	TEXT	5	prefix
fname	Learner's first name	TEXT	64	
mname	Learner's middle name/initial	TEXT	1	
lname	Learner's last name	TEXT	64	
gender	Learner's gender	TEXT	1	Either "M" or "F"
birthDate	Date of Birth (or Birth Day)	TEXT	10	YYYY-MM-DD format. If intent is to set only birth "day", set the YYYY value to "1900".
addressLine1	Learner's street address	TEXT	64	
addressLine2	Second line of learner's street address	TEXT	64	
city	Learner's city	TEXT	64	
state	Learner's state	TEXT	40	Expect 2-character state codes.
zip	Learner's ZIP code	TEXT	20	
country	Learner's country	TEXT	40	Expect 3-character ISO3 country code.
company	Learner's company/organization	TEXT	64	
jobTitle	Learner's job title.	TEXT	128	
professionId	Learner's profession ID	NUMERIC		Mapping file available upon request
phoneAreaCode	Learner's phone area code	TEXT	3	
phoneNumber	Learner's phone number	TEXT	15	
faxAreaCode	Learner's fax number area code	TEXT	3	
faxNumber	Learner's fax number	TEXT	15	
specialtyId	Learner's specialty ID	NUMERIC		Mapping file available upon request.

Name	Description	Data Type	Size Limit	Notes
degreeId	Learner's degree ID	NUMERIC		Mapping file available upon request
designation	Free-form list of (abbreviated) learner designations.	TEXT	64	
membershipId	Learner membership ID	TEXT	64	
npiNumber	NPI Number	TEXT	32	
boardNameId	Professional Association ID (Primary)	NUMERIC		Mapping file available upon request
boardNameId2	Professional Association ID (Secondary)	NUMERIC		Mapping file available upon request
boardNumber	Professional Association Number (Primary)	TEXT	32	
boardNumber2	Professional Association Number (Secondary)	TEXT	32	
siteCode	Site Code	TEXT	256	Available for reporting, but not displayed in learner facing profile form.
clientGroup	Client Group	TEXT	64	Available for reporting, but not displayed in learner facing profile form.
originUrl	Origin URL	TEXT	256	Available for reporting, but not displayed in learner facing profile form.
flexField1	Extended Learner Profile Field 1	TEXT	64	Customer "flex" field for extended profile form data. Form field label may be customized in learner profile form.
flexField2	Extended Learner Profile Field 2	TEXT	64	Customer "flex" field for extended profile form data. Form field label may be customized in learner profile form.
flexField3	Extended Learner Profile Field 3	TEXT	64	Customer "flex" field for extended profile form data. Form field label may be customized in learner profile form.

Name	Description	Data Type	Size Limit	Notes
`flexField4`	Extended Learner Profile Field 4	TEXT	64	Customer "flex" field for extended profile form data. Form field label may be customized in learner profile form.
`clientCustom1`	Client Custom 1	TEXT	64	Customer "flex" field for additional segmentation data. Available for reporting, but **not displayed in learner facing profile form**.
`clientCustom2`	Client Custom 2	TEXT	64	Customer "flex" field for additional segmentation data. Available for reporting, but **not displayed in learner facing profile form**.

How Trusted Handoff Profile Update Works

Rievent enables the customer to transmit a wide range of learner profile attributes as a component of a trusted handoff. The list of the available profile attributes are described in a preceding section of this document.

Learner Record of Participation

The Rievent Platform maintains separate database records for learner profile data at the activity participation, and overall learner account levels. The **learner participation record** can be thought of as a repository for learner activity participation and profile data at a particular slice in time, up to and until the activity is completed. The authentication provider, on behalf of the customer, determines what profile information shall be communicated through trusted handoff and added to the participation record profile.

During the trusted handoff validation process, existing profile data found for the associated learner account will be set into the participation record as a base profile when the record is created, followed by updating the record with handoff profile data exactly as provided by the referring site (applicably trimming to accommodate expected field size restrictions), including communicated empty values. Subsequent trusted handoff requests to the same activity with changed profile information will result in a corresponding change to learner profile information in the Rievent Platform. Rievent delegates responsibility to the authentication provider to determine how and what information is communicated to the participation record, and the validity of the information provided.

Profile Form Page

Following successful trusted handoff, the profile form component included in the activity will prompt the learner to update their profile if required profile parameters for the activity are missing in the handoff request and existing learner record. The customer instructs Rievent as to which profile form attributes are required.

Learner Account Profile

In addition to the learner participation record, Rievent also maintains a separate higher order learner account profile that is owned and maintained by the learner itself, and is intended to reflect the most current and up-to-date account information, and provides the basis for the information printed on the learner CE transcript. Profile information communicated by the authentication provider through trusted handoff is also propagated into the associated learner account profile. Once the learner profile has a complete set of required information, the learner will no longer be prompted by the profile form on subsequent activity participation. The learner may also update their account profile information at any time from within their account (My Profile) or from within the CE activity (Edit Profile link).

Exceptions and Special Cases to Profile Update

In order to prevent data corruption or removal of previously provided vital account profile information, there are some cases where data provided in the trusted handoff request is not exactly propagated to the learner account profile. There are increasing orders of rules and complexity that could be applied to govern how and when the learner profile is overwritten with external site data. Rievent has chosen to implement very basic prevention against updating (certain) learner account profile fields through trusted handoff with empty values as a basic means to preserve the integrity of previously provided profile data. As an example, once "name" information is provided, it cannot be removed from the learner profile by parameters (with empty values) communicated through a trusted handoff request, only replaced with non-empty values. The same applies to all address fields, with the exception of address line 2 which can be overwritten with an empty value.

How Entitlement Works

Rievent prefers to defer all entitlement determination to the customer. Understanding the potential for wide-ranging entitlement criteria, such as memberships, subscriptions, and/or prior purchase history, it is not practical to replicate and consult these types of information from within the Rievent Platform. As part of the SSO authentication process, Rievent relies on the customer to determine the learner's current entitlement status to the restricted resource (activity). If a learner is entitled to access the restricted components of the activity (content, post-test, credit), the customer will send the "`entitled=true`" claim as part of handoff token. Once the entitlement value is set to true in the Rievent Platform, the learner will continue to be provided access to the restricted components of the activity for the lifetime of the participation record.

Frequently Asked Questions

Question: What's the difference between all of the different learner identifiers such as externalId, membershipId, npiNumber, boardNumber? What data should we provide for each of these?

Rievent requires the `externalId` parameter be sent as part of the trusted handoff request. The value for this parameter should represent the unique identifier for the learner in your system of record. This value is used for creating a link between the two systems and is not something the learner will ever enter or modify themselves.

If you have another necessary attribute representing learner identity, membership, or entitlement, and one which the learner would have the ability to provide/modify themselves, the `membershipId` parameter would be a suitable candidate. It's only necessary or advisable to provide values for `npiNumber` or `boardNumber` if your learners are claiming ACCME and/or MOC credit.

Question: What data do we need to provide for the `professionId`, `specialtyId`, and `degreeId` fields? How do we know what ID values to provide?

The profession, specialty, and degree fields are optional components of the profile for which you can provide values and/or have the learner modify to meet your needs. The value provided in the `degreeId` field may be used to distinguish between Physician ("MD" and "DO") and Non-Physician (All Others) reporting for the ACCME, in lieu of the learner claiming one or the other types of credit. You may also find having data for these attributes useful for reporting and filtering. Rievent can provide spreadsheets containing our ID mappings for standard professions, specialties, and degrees.

Question: We are interested in keeping track of entry points to our learning activities. What values should we send for the `mct`?

A good start would be for you to describe the possible entry points to a learning activity. Rievent can create corresponding campaign tracker records in our platform, followed by providing you with the corresponding system IDs. You can then optionally provide the appropriate `mct` value in the trusted handoff request to identify point of entry which will build value and additional segmentation in your reporting.

Question: The "state" field size indicates that truncation occurs at 40 characters. Does this mean submitting a 2 character state code is optional? We have non-US learners, should we be submitting the full text value for our state field in this parameter (preferred), or instead should we leave the field blank?

Although the state field supports up to 40 characters, Rievent has a practical limitation of 2-character codes in an attempt to normalize US state values. There is actually room to hold larger values in the database but it is advised that state values are provided as 2-character codes for consistent reporting and learner profile experience. The value for state is optional and need not be provided when non-applicable, particularly for non-US learners.

Question: Is the 3 character ISO3 code format mandatory for country values? How does the 40 character limit apply?

Rievent has standardized reporting based on the expectation of ISO3 country codes. The learner profile form page will pre-select a value in a drop-down list based on the value for country being an ISO3 code.

Question: We store ISO2 codes in our system so if we needed to provide ISO3 codes we would require an additional translation process to convert these?

If an ISO2 code is provided, the learner profile form will present as if a value for country code were not on record. We recommend translating ISO2 to ISO3 codes as part of the trusted handoff request to Rievent.