U.S. Department of Transportation
Federal Motor Carrier Safety Administration

TRAINING PROVIDER REGISTRY

Web Services Development Handbook For Training Providers

Version 1.1

Prepared by:

Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

January 2021

Revision History

Revision Number	Document ID	Description of Change	Revision Date
1	Draft 1.0	Initial draft	July 2020
2	1.1	Updates to reflect the released version of the driver search service including testing access	January 2021

List of Definitions

Term	Definition
JSON	A data interchange format used to store object data as a string.
JSON Web Token (JWT)	A token composed as a JSON object for providing user authentication.
Public Key Certificate	A file containing the public key component of the public/private key pair along with expiration and issuance data.
Public/Private Key Pairs	Also known as asymmetric keys, public/private key pairs are used for encrypting and decrypting data, as well as signing and verifying electronic signatures. Public keys can be distributed to anyone who requests them, while private keys must be kept private and secure.
Service Private Key	A key issued by the TPR application that certifies the holder is the owner of the public/private key pair.
State	All of the States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, American Samoa, Guam, and the Virgin Islands.
Training Provider	An entity that is listed on the FMCSA Training Provider Registry. Training providers include, but are not limited to, training schools, educational institutions, rural electric cooperatives, motor carriers, State/local governments, school districts, joint labor management programs, owner-operators, and individuals.

List of Abbreviations

Acronym	Definition
AAMVA	American Association of Motor Vehicle Administrators
CDL	commercial driver's license
DOT	Department of Transportation
FMCSA	Federal Motor Carrier Safety Administration
ICD	Interface Control Document
JSON	JavaScript Object Notation
JWT	JSON Web Token
REST	Representational state transfer
SDLA	State Driver Licensing Agency
TPR	Training Provider Registry

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

This Web Services Development Handbook has been prepared by the Volpe National Transportation Systems Center (Volpe Center) for the Federal Motor Carrier Safety Administration (FMCSA) to guide and support training providers with the development of systems that will submit driver training certification data to the Training Provider Registry (TPR).

This handbook covers the following steps that training providers will need to take if they wish to use the TPR web service to submit data to the TPR:

1. Request a user account.
2. Register all locations where training is conducted.
3. Generate keys for interacting with the retrieval service.
4. Generate valid web service requests to the service.
5. Interpret the web service response.

Training providers will also have the option to manually enter data via the TPR web interface. Training providers that intend to use manual entry do not need to take the steps listed in this handbook, with the exception of registering in the TPR (when available).

1.2 About the TPR

FMCSA is partnering with the Volpe Center to design and develop the TPR web system. The TPR will be a secure online database that will allow State license examiners to determine if an entry-level driver has completed Federally-required training.

Once fully operational, the TPR will:

- Provide commercial driver license (CDL) applicants with the official list of providers from which they can receive entry-level driver training.
- Allow training providers to register to be added to this list and maintain their listing (training provider registration is scheduled to be available in summer 2021).
- Receive information from registered training providers certifying a driver's successful completion of entry-level driver training.
- Retain this driver training information and relay it to State Driver Licensing Agencies (SDLAs).

By Congressional mandate, the TPR must be fully operational by February 7, 2022.

1.3 Background

The Moving Ahead for Progress in the 21st Century Act (MAP–21) mandated that FMCSA issue regulations to establish minimum entry-level training requirements for interstate and intrastate CDL applicants obtaining a CDL for the first time; Class B CDL holders seeking an upgrade to a Class A CDL; and those seeking passenger (P), hazardous materials (H), or school bus (S) endorsements for the first time. FMCSA published the Entry-Level Driver Training (ELDT) final rule outlining the requirements for drivers, States, and training providers in the implementation of these training requirements. The ELDT final rule also mandated the development of the TPR to support the technical requirements of the ELDT regulations.

The main goal of the TPR is to improve safety on our Nation's roads by ensuring that all entry-level drivers receive comprehensive training from a self-certified training provider prior to obtaining a CDL, upgrade, or endorsement.

1.4 Roles and Responsibilities

FMCSA, training providers, drivers, and States all play important roles in the implementation of the TPR and the ELDT program. See the table below for a brief overview of these roles and responsibilities.

Table 1-1. Roles and Responsibilities

FMCSA	Training Providers	States	Drivers
• Develop and maintain the TPR database. • Approve provider and State user accounts. • Monitor the involuntary removal and reinstatement process for training providers.	• Register to create user account and provider listing. • Keep information in provider listing up to date. • Submit driver training certification information to FMCSA.	• Query TPR data to verify a driver's completion of required training before administering relevant tests.	• Search for training providers using the list on the TPR website. • Look up their training certification record by providing their identifying information.

2 Working with FMCSA

FMCSA is committed to working with our partners throughout the entire implementation process to assist them in registering with the TPR and support them in testing and debugging any programmatic interfaces to the TPR they choose to develop.

2.1 Register with FMCSA

To work with the TPR, training providers must register on the TPR website. The registration process will create your user account and submit your information, including provider name, contact information, location information, and types of training offered. This registration will be reviewed by FMCSA before being approved.

> ***Note: The ability to request an account is not currently available. This account is not required to begin testing (see Section 4 (Testing) for more details on accessing the testing service).***

2.2 Generate Service Access Credentials

Once a training provider's account request is approved, the training provider will then need to generate an access certificate to set up their web service interface. These credentials will consist of three parts:

- A unique identifier for the issued credentials.
- A certificate that will be used by FMCSA to verify that messages submitted by your service are coming from you.
- A private key that pairs with this certificate.

> ***Be sure to save this key and keep it protected as you would an account password. FMCSA will not maintain a copy of your private key. If you lose it, you will need to generate new credentials.***

You will be able to generate multiple sets of credentials and provide friendly names to allow for service endpoint identification, key transition, etc.

3 Submitting Training Data to FMCSA

FMCSA will provide a representational state transfer (REST) service to allow training providers to submit training data to the TPR. Request and response bodies will use JSON formatting.

Training providers will access the service using the credentials issued to the training provider by FMCSA to generate a JSON Web Token (JWT) and include this token in the request.

3.1 Authentication

All requests to the REST service will be secured using a JWT and bearer authentication. The token will be generated by the client (training provider) and signed using the key issued through the process described in section 2.2.

3.1.1 *Token*

When composing a request to the REST service, the client will need to generate a JWT with the following characteristics:

- Must use the RS256 signing algorithm.
- Must be signed using the private key generated in the process described in section 2.2 of this document.
- Payload must contain the following claims:
    - "nbf" (Not Before) – must be the current time or later with a 5 minute skew for clocks out of sync. The value must be provided as a Unix timestamp.
    - "exp" (Expiration) – must be no greater than 20 minutes after the "nbf" value and must not be in the past, plus a 5 minute skew for clocks out of sync. The value must be provided as a Unix timestamp.
    - "iss" (Issuer) – identifier for the credentials used to sign the token that has been issued by FMCSA in the generation process described in section 2.2.
- Payload may contain the following optional claim:
    - "sub" (Subject) – for tracking purposes the client may pass a local identifier which will be used to further identify actions performed by the service call. This value must be a URL encoded ASCII string with a maximum of 250 characters.

> *See RFC-7519 for the full JWT specification*

3.1.2 *Inclusion*

The JWT defined in 3.1.1 should be included in all service requests using the bearer authentication header. Specifically, a header should be included in the request with the key "Authorization" and value "Bearer <JWT Token>".

3.2 Responses

The TPR web service will notify the client of success or error using the HTTP response codes as defined in Table 3-1. Request Response Codes.

Table 3-1. Request Response Codes

Code	Description
201	Request was processed successfully and the training record was created.
400	The format of the request was invalid, details of the issue will be provided in a RFC 7807 compliant JSON response body.
401	Bearer JWT token was not found or was rejected. Details will be returned in the WWW-Authenticate. *Note: due to a current implementation limitation, authentication errors will appear in the x-amzn-Remapped-WWW-Authenticate header. We plan to resolve this issue in a future release.*
403	User was authenticated but tried to access a resource to which they did not have permission.
404	Requested resource was not found. In the case detail action, this would indicate that no driver information was found for the supplied id.
405	Incorrect verb was used when calling the action.
415	Content type header was excluded or not set to “application/json”.
500	Internal server error. Details of the issue will be provided in a RFC 7807 compliant JSON response body.

3.3 Training Submission

The training submission will allow the training provider to submit driver training certification data electronically to the TPR.

Endpoint: POST /api/Training/Add

3.3.1 *Request Body*

The request will contain one or more search parameters.

3.3.1.1 Elements

Table 3-2. Training Submission Body

Name	Description	Requirements
Number	Number used to identify a license or permit issued by the SDLA.	Up to 50 characters in length.
State	Country and State code as defined in ISO 3166-2.	Up to 6 characters using a 2-character country code, a dash, and a locality code of up to 3 characters.

Name	Description	Requirements
FirstName	Given name of the driver.	Up to 100 characters in length.
LastName	Surname of the driver.	Up to 100 characters in length.
DateOfBirth	Date in the ISO 8601 format including dashes to separate the components.	YYYY-MM-DD
ClassEndorsementCode	A code indicating the class/endorsements to which the training should apply.	One of: A, B, P, S, or H.
ApplicationType	Type of license the trainee is applying for when entering Class A or Class B.	Included for Class A and Class B submissions. One of: • New • Upgrade
ProviderLocationId	Unique identifier in the TPR for the location where the training was performed.	GUID in the format 00000000-0000-0000-0000-000000000000.
TrainingElements	An array of training elements.	An array of objects defined in Table 3-3. Training Element.

Table 3-3. Training Element

Name	Description	Requirements
TrainingType	Type of training represented by the entry.	One of: • Theory • PublicRoad • Range
CompletionDate	Date the user completed the training in the ISO 8601 format including dashes to separate the components.	YYYY-MM-DD
TrainingMethod	Method used for Theory Training.	Required for theory training. One of the values: • Online • Inperson Not included for public road or range.
Hours	Number of hours of training completed by the user.	Required for public road and range, not included for theory. Decimal value.
Score	Score received on the final test by the driver.	Required for theory, not included for public road or range. Integer between 80 and 100.

Name	Description	Requirements
InternalId	A local ID used to identify the training element in the training provider system. This value will be visible in the web UI, but will not be returned to the driver or State retrieving the data.	Optional String up to 255 characters in length.

3.3.1.2 Example

```
{
 "Number": "S1278908",
 "State": "US-MA",
 "FirstName": "John",
 "LastName": "Smith",
 "DateOfBirth": "1997-04-19",
 "ClassEndorsementCode": "A",
 "ApplicationType": "New",
 "ProviderLocationId": "c1d6ad9f-833c-4257-8e23-b1369ee09e8f",
 "TrainingElements": [
  {
   "TrainingType": "Theory",
   "CompletionDate": "2022-03-04",
   "TrainingMethod": "InPerson",
   "Score": 95,
   "InternalId": "TPREC-123456"
  }
 ]
}
```

Figure 3-1. Example theory training submission body

```
{
 "Number": "S1278908",
 "State": "US-MA",
 "FirstName": "John",
 "LastName": "Smith",
 "DateOfBirth": "1997-04-19",
 "ClassEndorsementCode": "A",
 "ApplicationType": "New",
 "ProviderLocationId": "43887859-6552-4c6e-b13f-f0411b5b9150",
 "TrainingElements": [
  {
   "TrainingType": "Range",
   "CompletionDate": "2022-05-04",
   "Hours": "10",
   "InternalId": "TPREC-987654"
  }
 ]
}
```

Figure 3-2. Example behind the wheel training submission body

3.3.2 *Response*

A status 201 response will contain an RFC 7807 compliant response if the submission caused a warning. Otherwise, no response body will be returned.

4 Testing

Access to the TPR service has been made available at the main TPR domain, tpr.fmcsa.dot.gov. Requests must be made over https, http requests are not supported. This same endpoint will be used for test submissions to the service.

All necessary testing files are posted to TPR Developer's Toolkit.

4.1 Credentials

Three certificates and private keys stored in a pfx file are available in the "Testing credentials" package of the TPR Developer's Toolkit:

- Provider.pfx – contains an active non-expired certificate and key
- Provider -Expired.pfx – contains an active but expired certificate and key
- Provider -Revoked.pfx – contains a non-expired certificate that has been marked 'revoked' in the system

Identifiers for each of these certificates are included in the "Issuers.txt" file. The appropriate issuer identifier should be included in the "iss" claim of the signed JWT when submitting it to the service.

Note: At this time the service only supports test submissions using the test credentials above. Once the production service is available, and States have their service access credentials, the credentials used when submitting a request will determine if the request accesses production or test data.

4.2 Known Issues/Potential Enhancements

- As noted in Section 3.2, a 401 response should provide error details on the "WWW-Authenticate" header. Due to current implementation constraints, it is returned on the "x-amzn-Remapped-WWW-Authenticate" instead. We plan to resolve this issue in a future release and will update this handbook when this occurs.

Appendix A: Additional Resources

This section provides some of the resources and documents that are most closely related to or referenced within this document, such as the Final Rule.

- Training Provider Registry
- 49 CFR Part 380 Subpart F: Entry-Level Driver Training Requirements On and After February 7, 2020
- 49 CFR Part 380 Subpart G: Registry of Entry-Level Driver Training Providers
- 49 CFR § 383.71: Driver Application and Certification Procedures
- 49 CFR § 383.73: State Procedures
- 49 CFR § 384.230: Entry-Level Driver Certification
- Guidance on developing JSON Web Tokens can be found at JWT.io
- Contact information for submitting questions and comments to the TPR development team: https://tpr.fmcsa.dot.gov/#contact

Appendix B: References

Organization	Standard	Purpose
International Standards Organization (ISO)	ISO 3166-2	Used to define State codes in driver searches and search results.
	ISO 8601	Format used for encoding dates.
Internet Engineering Task Force	RFC 7797	Definition of the JSON Web Token used to authenticate requests.
	RFC 7807	Define standard error responses for REST API.
	RFC 6750	Define details of bearer authentication process and error handling.
	RFC 2616	HTTP verb and response code definitions.

Federal Motor Carrier Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

855-368-4200
www.fmcsa.dot.gov

John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov

U.S. Department of Transportation
Federal Motor Carrier Safety Administration