Attachment 16

OSCAR
Overview

Background

The One Stop Credentialing and Registration (OSCAR) service is a java, web-based application developed and maintained by the NYS Department of Taxation and Finance for interstate carriers to obtain International Registration Plan (IRP), International Fuel Tax Agreement (IFTA) and Highway Use Tax (HUT) credentials. The OSCAR system interacts with the three state agencies which are administer these credentials – Department of Transportation, Department of Tax and Finance and the Department of Motor Vehicles.

The OSCAR system provides the following on-line functionality to carriers and service companies acting on behalf of carriers:

- Enroll as on-line customers,
- Apply for credentials,
- Modify fleet and credential information,
- Make electronic payments for credentials, and
- Receive credentials

Through interfaces with the participating agencies, OSCAR provides verification of carrier identification and vehicle information.

This Document

This document provides prospective vendors with a summary description of OSCAR’s system, interfaces and related information. It is not all-inclusive.
DTF Enrollment Process
This diagram illustrates how a new carrier enrolls with OSCAR.
Passing User From DTF to DOT

1. Once the user is ready to transfer to the DOT site, DTF returns a self-submitting HTML page back to the user's browser, instructing it to "POST" the HTML page to a DOT URL. The page is pre-populated with an encoded SAML Assertion (as one of the page's fields that will be "posted") that identifies the user. The SAML *Assertion will also contain the security credentials (ID and Password) of DTF. The security credentials should be for a "service account" created at DOT for DTF. (This can/will be adjusted for DOT's security requirements/environment).

   *contains a user id and password for a service account created at DOT, the “DOT customer number” (previously referred to as a “DOT account number”), OSCAR transaction ID, Service Bureau ID / Carrier ID, and an indicator for type of account, and an indicator for type of business being performed.

The self-submitting HTML page sent back to the user's browser will be passed over Secure Sockets Layer (SSL), and then the page will "POST" to DOT's URL over SSL. DOT will need to be able to accept SSL traffic.

2. DOT's target web server accepts only HTTPS traffic. (Any traffic to the URL that does not have HTTPS is rejected).

3. DOT's target servlet "filter" (behind the web server) consumes the SAML assertions, meaning that they are not stored anywhere for re-use. The SAML Assertion is decrypted, DTF is authenticated, the user is identified (the user information can be stored), and then the SAML Assertion is discarded.

Connectivity Specifications

Calling DTF Web Service From DOT to confirm System Availability

1. Once the user is ready to pay, DOT makes a web service call to DTF to confirm System Availability prior to transferring the user over to OSCAR.

2. DOT POSTs a SOAP message to DTF and DTF replies with a SOAP message. The messages following a WSDL specification DTF provides. DTF also provide 3 URL's for DOT to POST to: one for DVM, UTM and Production.

3. SOAP messages are passed over the internet via a Secure Sockets Layer (SSL).

4. DTF's target web server accepts only https traffic. (Any traffic to the URL that does not have https is rejected.)

5. Any calls to DTF's web service should come from a specific IP subnet (DOT's subnet). Calls from any other subnet will be denied.

6. Calls to DTF's web service will need another means of network level security for authentication (details are yet to be confirmed).
Passing User From DOT to DTF

1. Once the DOT user has completed their work on the DOT Permitting System, DOT will transfer control to DTF by returning a self-submitting HTML page back to the user's browser, instructing it to "POST" the HTML page to a DTF URL. The page is pre-populated with an encoded SAML Assertion (as one of the page's fields that will be "posted") that identifies the user. The SAML *Assertion will also contain the security credentials (ID and Password) of DOT. The security credentials should be for a "service account" created at DTF for DOT.

*contains the security credentials (ID and Password) of DOT, the OSCAR transaction ID, and the amount to be charged.

The self-submitting HTML page sent back to the user's browser is passed over Secure Sockets Layer (SSL), and then the page is "POSTed" to DTF's URL over SSL. DTF will need to be able to accept SSL traffic.

2. DTF's target web server needs to accept only HTTPS traffic. (Any traffic to the URL that does not have HTTPS is rejected)

3. DTF's target servlet "filter" (behind the web server) consumes the SAML assertions, meaning that they are not stored anywhere for re-use. The SAML Assertion is decrypted, DOT is authenticated, the user is identified (the user information can be stored), and then the SAML Assertion is discarded. The authentication of DOT's service account is done via an LDAP-bind to the State-wide LDAP.

Calling DOT Web Service From DTF to Acknowledge Payment Made

1. Once the user completes payment through OSCAR, DTF makes a web service call to DOT to communicate the information.

2. DTF POSTs a SOAP message to DOT and DOT replies with a SOAP message. The messages will follow WSDL specifications provided by DOT.

3. SOAP messages are passed over the internet via a Secure Sockets Layer (SSL).

4. DOT's target web server will accept only HTTPS traffic. (Any traffic to the URL that does not have HTTPS should be rejected)

5. Any calls to DOT's web service should come from a specific IP subnet (DTF's subnet). Calls from any other subnet will be denied.

6. Calls to DOT's web service will need another means of network level security for authentication (Still waiting to hear from DOT...we need to know more about their security capabilities/systems before we can recommend a solution).
OSCAR TRANSFERS USER TO DOT
*using the Browser/POST Profile as defined in SAML v1.1

1. User navigates to OSCAR homepage and enters login information. User is authenticated and logged in using OSCAR's current authentication.

2. User selects link to do DOT business which redirects them to OSCAR's Inter-Site Transfer Service (ISTS) page by POST'ing a form to it.

3. OSCAR's Inter-Site Transfer Service (ISTS) page constructs a SAML assertion from the Service Bureau info from the info passed in from the POST, then in turn POST's the SAML *assertion to the External Application target URL (DOT) over a Secure Sockets Layer (SSL).
   *contains a user id and password for a service account created at DOT, the "DOT customer number" (previously referred to as a "DOT account number"), OSCAR transaction ID, Service Bureau ID / Carrier ID, and an indicator for type of account, and an indicator for type of business being performed.

4. DOT's Assertion Consumer (which is a Servlet Filter that protects the application's gateway servlet) grabs the user id and password for the service account, the "DOT customer number", the OSCAR transaction ID, Service Bureau ID and the type of account indicator. DOT's Assertion Consumer will authenticate DTF with the user id and password. Once the user is identified, the servlet will store the DOT account number, the OSCAR transaction ID, Service Bureau ID and the type of account indicator in the session and then allows the request to go to the target (the Application Home).

* The red lines in the above diagram represent communication over a Secure Sockets Layer (SSL).
1. Phase 1 - User has already logged in through OSCAR and has been transferred over to DOT’s External Permitting System.
2. (optional) The External Permitting System initiates a web service call over SSL to DTF to confirm that OSCAR and the Credit Card Server are “up” and available.
3. User selects link to pay by Credit Card which redirects them to the DOT Inter-Site Transfer Service (ISTS) page.
4. DOT’s Inter-Site Transfer Service (ISTS) page constructs a SAML assertion and then POSTs the SAML assertion to the External Application target URL (DTF) over a Secure Sockets Layer (SSL).
5. DTF’s Assertion Consumer (which is a Servlet Filter that protects the application’s gateway servlet) grabs the user id and password for the service account, the OSCAR transaction ID, and the amount to be charged. DTF’s Assertion Consumer will authenticate DOT with the user id and password. Once the user is identified, the servlet will store the OSCAR transaction ID, and the amount to be charged in the session and then allows the request to go to the target (the Credit Card Payment Screen).
6. The application server attempts to process the credit card payment and upon confirmation of payment then processes and stores the transaction data. At this point DTF performs a web service call over SSL to DOT confirming that payment was received. After the web service call is complete, the user will be transferred to the Confirmation Page.

* Denotes Secure Sockets Layer (SSL)
**OSCAR Hours of Operation**

Support Phone Number: 518-474-7667  
Email Support at: [OSCAR_Webmaster@tax.state.ny.us](mailto:OSCAR_Webmaster@tax.state.ny.us)

<table>
<thead>
<tr>
<th>Day</th>
<th>Hours of Operation</th>
<th>Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>Opening at 12am</td>
<td>8:30am – 4:30pm</td>
</tr>
<tr>
<td>Tuesday</td>
<td>All Day</td>
<td>8:30am – 4:30pm</td>
</tr>
<tr>
<td>Wednesday</td>
<td>All Day</td>
<td>8:30am – 4:30pm</td>
</tr>
<tr>
<td>Thursday</td>
<td>All Day</td>
<td>8:30am – 4:30pm</td>
</tr>
<tr>
<td>Friday</td>
<td>All Day</td>
<td>8:30am – 4:30pm</td>
</tr>
<tr>
<td>Saturday</td>
<td>Closing at 8:45pm</td>
<td>None</td>
</tr>
<tr>
<td>Sunday</td>
<td>Closed</td>
<td>None</td>
</tr>
</tbody>
</table>

---

**Central Permits Office External Permits Automation Hours of Operation**

Support Phone Number: 518-485-2999, OR 1-888-783-1685  
Email Support at: [SpecHaul@dot.state.ny.us](mailto:SpecHaul@dot.state.ny.us)

<table>
<thead>
<tr>
<th>Day</th>
<th>Hours of Operation</th>
<th>Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>Opening at 12am</td>
<td>7:00am – 5:00pm</td>
</tr>
<tr>
<td>Tuesday</td>
<td>All Day</td>
<td>7:00am – 5:00pm</td>
</tr>
<tr>
<td>Wednesday</td>
<td>All Day</td>
<td>7:00am – 5:00pm</td>
</tr>
<tr>
<td>Thursday</td>
<td>All Day</td>
<td>7:00am – 5:00pm</td>
</tr>
<tr>
<td>Friday</td>
<td>All Day</td>
<td>7:00am – 5:00pm</td>
</tr>
<tr>
<td>Saturday</td>
<td>Closing at 8:45pm</td>
<td>None</td>
</tr>
<tr>
<td>Sunday</td>
<td>Closed</td>
<td>None</td>
</tr>
</tbody>
</table>

---

**DOT Help Desk Support Hours of Operation**

Support Phone Number: 518-485-8111, OR 1-888-644-9343  
Email Support at: [Helpdesk@dot.state.ny.us](mailto:Helpdesk@dot.state.ny.us)

<table>
<thead>
<tr>
<th>Day</th>
<th>Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>6:00am – 6:00pm</td>
</tr>
<tr>
<td>Tuesday</td>
<td>6:00am – 6:00pm</td>
</tr>
<tr>
<td>Wednesday</td>
<td>6:00am – 6:00pm</td>
</tr>
<tr>
<td>Thursday</td>
<td>6:00am – 6:00pm</td>
</tr>
<tr>
<td>Friday</td>
<td>6:00am – 6:00pm</td>
</tr>
<tr>
<td>Saturday</td>
<td>None</td>
</tr>
<tr>
<td>Sunday</td>
<td>None</td>
</tr>
</tbody>
</table>