OSBI RAPUP Interface

* The system shall interface with OSBI’s new Record of Arrest and Prosecution Update Portal (RAPUP). The integration will be bi-directional. This interface should search, display, and import arrest information from RAPUP and submit final disposition data in real-time.

This interface is expected to significantly improve the disposition submission rate by leveraging the workflow engine available in a modern PCMS. The OSBI’s new Record of Arrest and Prosecution Update Portal (RAPUP), is currently being developed by the SEARCH Open Justice Broker Consortium (OJBC) to replace the paper process currently employed by many small and medium-sized municipal courts. The OSBI is now expanding RAPUP’s functionality to push fingerprint-based arrest data into DA PCMSs, resulting in more efficient updating of arrest outcomes for state charges, including felonies, misdemeanor crimes of domestic violence, and other criminal events. Integration of arrest information either directly from Livescans or from the repository into DA PCMSs will also create notifications to request that defendants charged with reportable offenses be remanded for collection of fingerprints when not previously taken. This addresses the problem of missing OTN data attributed to so-called “cite-and-release” and other instances of criminal defendants being charged without updating the state’s criminal history record repository. RAPUP will also provide an interface for real-time validation and synchronization of OTNs and charging language variations. By implementing a modernized interface with the OSBI and leveraging the built-in workflow engine, the DAs will be able to automatically and accurately flag dispositions for submission to the OSBI.

This interface provides a secure outbound interface to import OTN and other arrest information from OSBI’s Computerized Criminal History (CCH). The interface must be able to invoke RAPUP’s Rest API/webservice by submitting known defendant information. A SAML authentication will be used to pass user information. A successful transaction should return one or more matching arrest records. The PCMS must provide an intuitive user interface to allow users to review and act on the information. If an arrest is selected, the PCMS must update the Offender Tracking Number and Charge UID on the defendant’s record. The WSDL for this service will be provided. The PCMS must also have an automated process to invoke a call to submit court disposition and sentencing information to RAPUP.

Data Elements

The primary data elements:

* Defendant pedigree information
	+ Person’s names and identifying numbers
	+ Date of birth
	+ Height, weight, hair/eye color – physical characteristics
	+ Contact information – addresses, phone numbers, email, etc.
	+ Optionally – aliases, gang information, mug shot, etc.
* Charges (collection)
	+ Incident date & time
	+ Incident location
	+ Charge and statute codes
	+ Charge description
	+ Severity
* Arrest information
	+ Date & Time
	+ Booking Officer
	+ Person Booked
	+ Offender Tracking Number
* Court Disposition & Sentencing Information
	+ Incident date & time
	+ Incident location
	+ Charge and statute codes
	+ Charge description
	+ Severity

Search Interface

1. The RAPUP webservice interface will allow a look-up on arrest by OTN or by providing a first name, last name, court case number and ORI. (users must provide all of this information before they can conduct a search).
2. After the search is complete, the interface will return a list of matching arrests to PCMS.
3. The PCMS end-user will select and import the OTN and Charge UID information from the result of arrest records.

Disposition Submission

1. The PCMS will have an automated workflow process to identify and flag cases for OSBI submission.
2. Once a case is flagged for submission to OSBI, the PCMS will invoke a Rest API/Webservice provided by RAPUP to submit the court outcome/final disposition in real-time.

# Oklahoma RAPUP Service Integration Specifications

## Overview

Oklahoma has developed a disposition reporting tool and portal that allows users to add, edit and delete dispositions to arrest charges. This helps provide a more accurate Criminal History record and give agencies the ability to manage arrests and dispose of charges properly.

In addition to allowing users the access to do this by using a portal, the RAPUP tool will also integrate with 3rd party case management systems using web services. This document will describe the integration specifications and authorization requirements.

## Web Service Operations and Messaging

### **Asynchronous Operations**

All web services provided by RAPUP are asynchronous service pairs. The client will send a one-way message to the server using a request web service operation. The server will then reply to a service that the client hosts using a response web service operation. The Message ID contained in the WS Addressing Soap header will be used to correlate request and response messages by the client.

### **Criminal History Search Services**

There are existing services that allow for searches on District Attorney (DA) and Municipal Court arrest, charges and dispositions. The service specifications can be found on GitHub.com:

Criminal History Search Request Service WSDL:
<https://github.com/ojbc/main/blob/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Search_Request/schema/SIP_WS_1.2/Criminal_History_Search_Request_Service.wsdl>

Criminal History Search Response Service WSDL:

<https://github.com/ojbc/main/blob/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Search_Results/schema/SIP_WS_1.2/Criminal_History_Search_Results_Service.wsdl>

The GitHub folders also link to sample invocation messages:

<https://github.com/ojbc/main/tree/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Search_Request/artifacts/service_model/information_model/IEPD/xml>

<https://github.com/ojbc/main/tree/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Search_Results/artifacts/service_model/information_model/IEPD/xml>

After a search is performed, results are returned that can also include deferred dispositions. The system can then modify these records by invoking Criminal History Modification Services which are described in the next section.

### **Criminal History Modification Services**

Once a Criminal History Search is completed and arrest and charges are returned, accompanying dispositions can be added, edited or deleted. The web services to do so are also on GitHub:

Criminal History Modification Request Service WSDL:

<https://github.com/ojbc/main/blob/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Modification_Request/schema/SIP_WS_1.2/Criminal_History_Modification_Request_Service.wsdl>

Criminal History Modification Response Service WSDL:

<https://github.com/ojbc/main/blob/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Modification_Response/schema/SIP_WS_1.2/Criminal_History_Modification_Response_Service.wsdl>

The GitHub folders also link to sample invocation messages:

<https://github.com/ojbc/main/tree/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Modification_Request/artifacts/service_model/information_model/IEPD/xml>

<https://github.com/ojbc/main/tree/master/shared/ojb-resources-common/src/main/resources/ssp/Criminal_History_Modification_Response/artifacts/service_model/information_model/IEPD/xml>

The following operations are supported in the RAPUP application:

* ReferChargeRequest
	+ Used to refer a charge
* FinalizeArrestRequest
	+ Used to mark an arrest record as complete so no more changes can be made.
* ReferArrestRequest
	+ Used to refer all charges in an arrest.
* DeclineChargeRequest
	+ Used to add a disposition of “charge declined” to an existing charge.
* ExpungeRequest
	+ Used to expunge an arrest.
* ModifyArrestRequest
	+ Used to add or edit a disposition to a charge on an arrest.

## Authentication and Authorization

The system-to-system services will be secured using mutual certificate authentication and SSL. The server will provide a server-side SSL certificate and during the handshake, the client will provide a certificate that is trusted by the server. The client and server will agree on what ciphers are allowed and the appropriate key sizes. All certificates will either be self-signed or provided by a free 3rd party provider such as Let’s Encrypt (<https://letsencrypt.org/>)

Even though the invocations are system to system, there will need to an audit trail to identify what users are performing what operations. This may not be applicable if an operation is performed as part of a batch process. However, when a service is invoked based on a user action, the user will need to be identified for audit purposes. The mechanisms to do this for system-to-system interactions will be determined in the future but existing services user to system services use Security Assertion Markup Language (SAML).

## Additional Services to be Developed

The following services will also be developed jointly as part of integrating with CMS’s:

* Develop a web service that allows Municipal Court and District Attorney case management systems to request Arrest/OTN information from the CCH database.
* Develop a web service that allows Municipal Court and District Attorney to request arrests missing dispositions.
* Develop a web service that allows Municipal Court and District Attorney case management systems to validate OTN and retrieve charge details, per that OTN.