CCMS Data Exchange Common Technical Requirements Document

FEBRUARY 2012

INFORMATION SERVICES DIVISION
ADMINISTRATIVE OFFICE OF THE COURTS

ADMINISTRATIVE OFFICE OF THE COURTS

INFORMATION SERVICES DIVISION

Judicial Council of California
Administrative Office of the Courts
Information Services Division
455 Golden Gate Avenue
San Francisco, California 94102-3688
415-865-4200
www.courts.ca.gov

Communications Team

This document was prepared by:

Edmund Herbert
California Administrative Office of the Courts
Information Services Division – Data Integration Program
455 Golden Gate Ave.
San Francisco, CA 94102-3688
Office 415-865-5336

Daniel Wu
California Administrative Office of the Courts
Information Services Division – Data Integration Program
455 Golden Gate Ave.
San Francisco, CA 94102-3688

Revision History

Version	Date	Description of Changes
1.0	12/1/2010	First release
2.0	09/10/2011	Added Global Channel Updated Court Code Explained Correlation ID Added Source and Target IDs
2.0.1	11/23/2011	Removed Source and Target IDs
2.0.2	12/22/2011	Added SOAP Header UNT example: Appendix C Added OWSM WSDL Policy: Appendix C

Reference Documents

Version	Date	Document Title	Author
1.0.0	12/10/10	Integrated Services Backbone Connectivity Testing Guide	AOC

Table of Contents

List of Figures

List of Tables

1.0 Overview

1.1 *Purpose*

The purpose of this document is to provide integration partners with useful technical information in preparation for implementing data exchanges with the California Court Case Management System (CCMS). This document outlines the technical requirements set out by the Administrative Office of the Courts (AOC), which must be adhered to by integration partners in order to participate in the exchange of data with the courts. It provides a series of steps to assist integration partners and the AOC in validating the readiness of an integration partner to participate in the secure exchange of data with CCMS.

1.2 *CCMS Data Exchange Overview*

As part of the CCMS project, 121 data exchanges servicing all case types have been developed to enable courts and their integration partners to exchange information using CCMS. Sixty-three exchanges are based on data exchange standards established in the National Information Exchange Model (NIEM), whereas 58 exchanges are based on CCMS XML schema. It is important to note that each of the 121 exchanges is actually a set of exchanges that includes individual exchanges for Request, Response, and Error Handling. A complete list of CCMS data exchanges is available on the Integration Partners website[1].

1.3 *Audience*

This document is intended for individuals who need to understand how a data exchange works in order to implement that exchange between the integration partner and CCMS. The current known audience includes:

- Integration Partner CCMS Data Exchange Implementation Team
- AOC Data Integration Program staff (business analyst, developer, architects, etc.)
- Integrated Services Backbone (ISB) vendors
- CCMS vendors
- Court CCMS project managers and subject matter experts (SMEs)

[1] http://www.courts.ca.gov/partners/integration.htm

2.0 Common Data Exchange Requirements

The current recommended data exchange message size limit is 10Mb. For specific data exchanges there may be exceptions to the message size limitation. Please see the exchange-specific Service Description Documents (SDDs) for these exceptions. The SDDs are available on the Integration Partners website.

3.0 Technical Requirements

3.1 *Connectivity*

A secure connection is required for all inbound and outbound data exchanges. Integration partners must use either TLS (Transport Layer Security) or its predecessor SSL (Secure Socket Layer) communication protocols.

- HTTPS, SFTP, and FTPS.
- All certificates of authority in use must be from a commercial CA. Self-signed certificates are not permitted.
- If transport encryption cannot be supported by an integration partner, payload encryption must be implemented according to California Courts Technology Center (CCTC) security policies.
- Integration partners should test HTTPS connections by connecting to the connectivity test web page at https://isb-dx.tst.courts.ca.gov/soa-infra/services/default/PartnerConnectivityComposite/PartnerConnectivityService.
- More information is available in the *Integrated Services Backbone Connectivity Testing Guide.*

3.2 *Authentication*

Integration partners may implement and consume data exchanges using Web Services and/or FTP transport protocols. Irrespective of the transport protocol, specific security measures are in place to correctly identify and authenticate consumers of CCMS data exchanges. Partners must use the credentials provided by the AOC to invoke data exchanges at the California Courts Technology Center (CCTC).

- The AOC/CCTC Operations Team will create integration partner username/password credentials.
- The integration partner is provided with the specific username/password credentials to be used for data exchange Web Services.
- The integration partner's application must generate user/password tokens.
- The UNT (Username Token) header is not part of the exchange packages distributed on the Integration Partners website. Partners should use the UNT security header shown in Appendix C for authentication. More information is available in the Integrated Services Backbone Connectivity Testing Guide.
- The Web Service: https://isb-dx.tst.courts.ca.gov/soa-infra/services/default/PartnerConnectivityCompositeNoAuth/PartnerConnectivityServiceNoAuth is available to integration partners to test credentials.

- For outbound exchanges where the integration partner hosts the Web Service, the partner will provide the AOC with the credentials for authenticating on their system. Similar to AOC, the integration partner can provide the AOC with a test URL for the AOC to authenticate these credentials.

3.2.1 FTP transport protocol

- The only permissible inbound FTP transport types at the CCTC (in order of preference) are:
  - SFTP - FTP over SSH with PGP file encryption.
  - FTPS - FTP over SSL (Explicit Invocation Mode) with PGP file encryption.

- Inbound FTP transactions require the following components:
  - FTP user name and password
  - Source IP, PGP keys
  - SSL certificates of authority (if FTP over SSL is used.)

  Note: Anonymous FTP access or use of anonymous as the user name and/ or password is prohibited.

- Obtain AOC/CCTC Enterprise FTP credentials. Integration partners will need to obtain username and password credentials if the CCTC Enterprise FTP server will be used as the data exchange point.
- The integration partner will provide username/password credentials to be used by the AOC to push/pull from integration partner's FTP server.
- The AOC and integration partner will adhere to each other's password policies.

3.3 *Payload Encryption*

- Payload encryption is focused on the data itself rather than the transport. Data at rest is encrypted using tools such as PGP or open-PGP, prior to transporting the data to another system. Once the data is delivered it remains encrypted until the recipient decrypts the data.
- The CCTC supports encryption adhering to Open-PGP or PGP specifications.
- All encryption must comply, at a minimum, with the AES-128 standard. The CCTC also supports the AES-256 encryption standard.
- When the CCTC Enterprise FTP server is used as the data exchange point then payload encryption is required as the data will be stored in the DMZ (accessible by the public.)

3.4 *Integrated Services Backbone*

- The Integrated Services Backbone (ISB) provides four schemas for use with data exchanges between integration partners and the courts. The layout of the schemas along with data element definitions is shown in Figure 1 and Figure 2.

- Three of the ISB schemas are header type schemas. They contain specific values for exchange request (initiation) type messages as well as for exchange response (Success or Error) type messages.
- Integration partners should plan to test the ISB headers in conjunction with data exchange payload content testing.
- Integration partners should also plan to host a notification service for use when errors are encountered on the ISB while processing an asynchronous data exchange bound for the CCMS system. The AOC provides the specification for this notification service.

Figure 1and Figure 2 show the use of the three ISB header schemas for integration partner-initiated synchronous and asynchronous data exchanges, respectively.

3.4.1.1 Synchronous Data Exchange

In a synchronous data exchange, the integration partner initiates the data exchange by sending a request to the ISB. The ISB maintains the connection to send the business response back to integration partners.

Upon receiving the request, the ISB validates the WSDL and data exchange payload. If the validation fails, the ISB sends a “Common Error Message” back to the integration partner system, or if successful the payload is transformed into CCMS format and forwarded to the CCMS system. If payload transformation fails or the ISB is not able to forward the data to CCMS, the ISB sends a “Common Error Message” back to the integration partner.

CCMS performs the business operation and returns a business response back to the ISB, which validates, transforms, and forwards the response back to the integration partner.

Note:

- Sending the “Common Error Message” back to the integration partner is optional.
- The request sent from the integration partner and the response sent by the ISB occurs within the single connection established by the integration partner as shown in Figure 1.

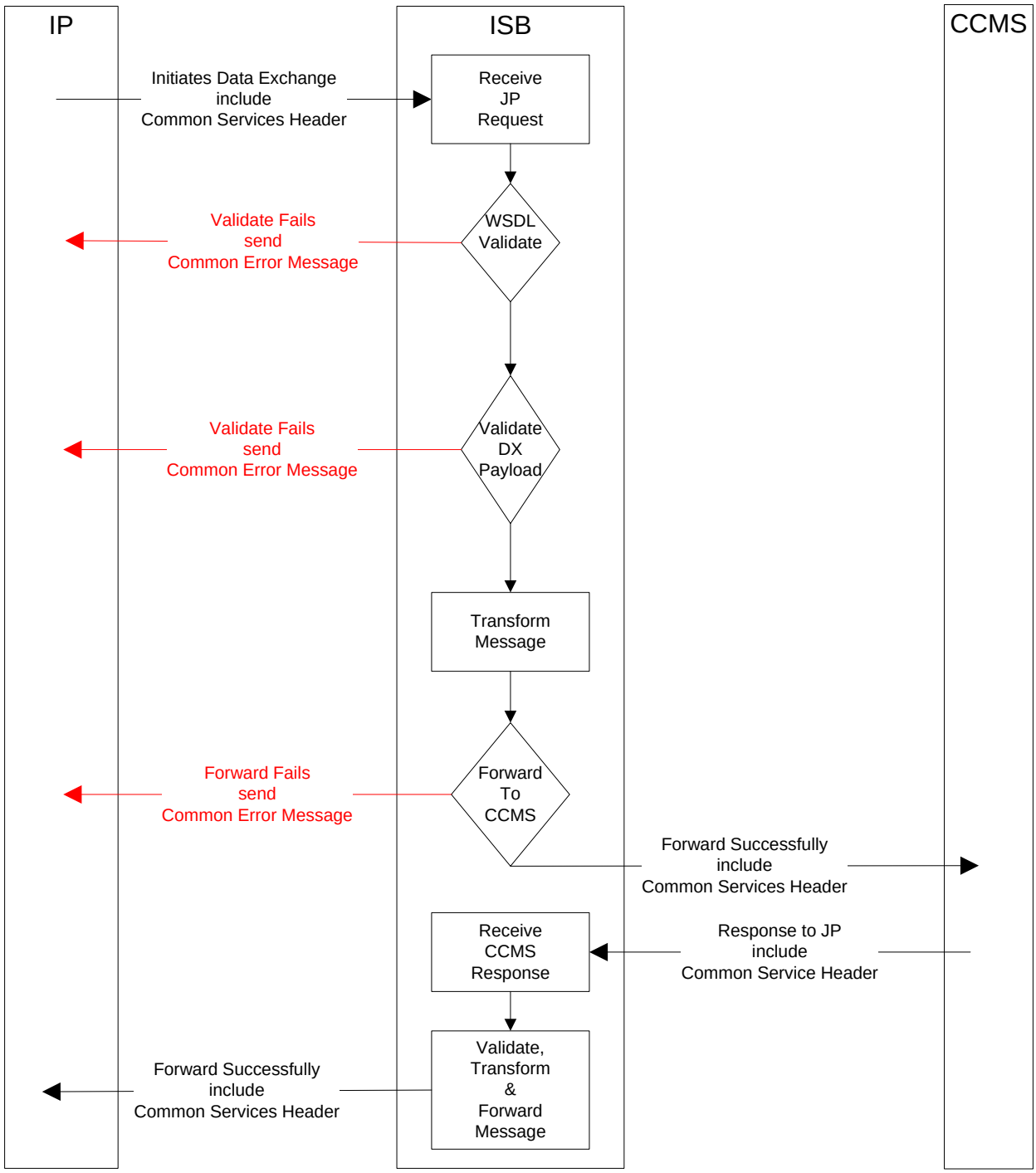

Figure 1. Use of the ISB Header Schemas for Synchronous Data Exchanges

3.4.1.2 Asynchronous Data Exchange

In an asynchronous data exchange the integration partner initiates data exchange and sends data to ISB. The ISB validates the WSDL and responds with an acknowledgement (ACK) to the integration partner to indicate that the data was received successfully. If WSDL validation fails, the ISB sends a "Common Error Message". At this point, the request transaction is complete and the integration partner's Data Exchange Response Service waits for a response from the ISB.

The ISB continues processing the request. It validates the data exchange payload, transforms the data to CCMS format, and forwards the request to CCMS. If the data exchange payload validation or forward to CCMS fails, the ISB can send a "Common Error Message" back to the integration partner. This message can be consumed by integration partners only if a notification service is implemented and is listening to ISB messages. Running a Notification Service is optional, but the AOC recommends partners run this service as it provides additional information regarding the status of the request. Details about the notification are provided in section 3.4.1.9.

CCMS performs a business operation and sends the response to the ISB, which transforms the data and forwards the response to the integration partner's Data Exchange Response Service.

As shown in Figure 2, the transactions happen in three stages in an asynchronous data exchange:

- Integration partner sending request to ISB and waiting for response
- ISB sending notification service to the integration partner's Notification Service
- ISB sending business response back to the integration partner's Data Exchange Response Service

Correlation ID:

As asynchronous data exchanges allow integration partners to send multiple requests and wait for response from the ISB, a Correlation ID is used for uniquely identifying the response. The Correlation ID is provided by the source (integration partner). All asynchronous exchanges need a Correlation ID except for EFL902 - Send Clerk Review Rejection Notification.

Note: Sending a "Common Error Message" back to the integration partner is optional.

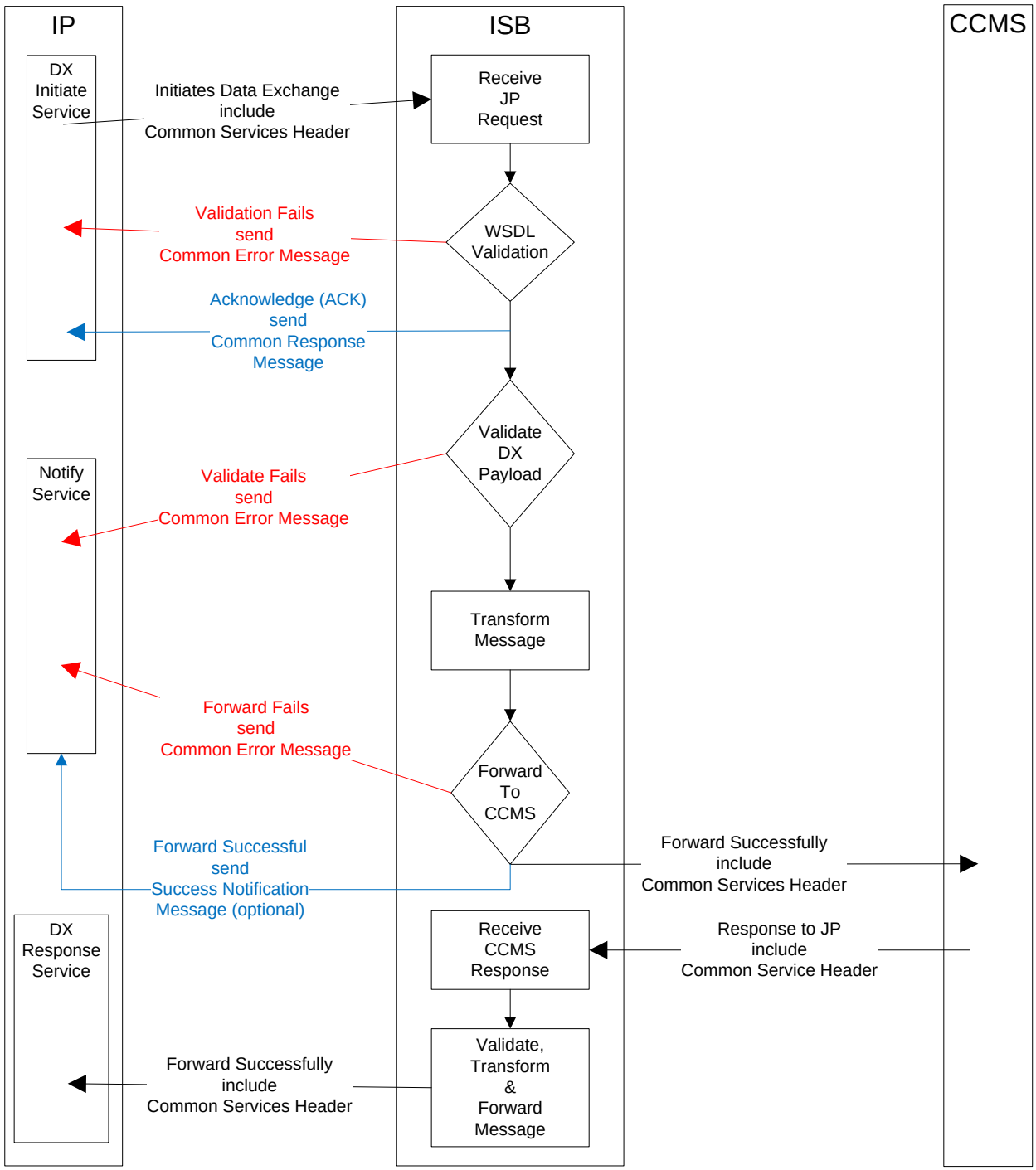

Figure 2. Use of the ISB Header Schemas for Asynchronous Data Exchanges

3.4.1.3 Common Service Header schema

This schema is used as the header for all data exchange business request and functional response type messages. Integration partners are responsible for populating the required elements in this schema prior to invoking the data exchange in both request and response scenarios. This message header type schema is used in the following four scenarios:

1. When there is an inbound data exchange message from the integration partner to the court.
2. When there is an outbound CCMS functional success or error response message from the court to the integration partner.
3. When there is an outbound data exchange message from the court to the integration partner.
4. When there is an inbound functional success or error response message from the integration partner to the court.

The Common Service Header is located in the "ISBCommonServiceHeader.xsd" schema file. Table 1 provides descriptions of the Common Service Header schema element names.

Table 1. Common Service Header Schema Element Names

Element Name	Description	Required
Source	Unique identifier for the source system. The AOC will provide this unique value for all integration partner systems. The integration partner source system is then required to include this value in this element for all data exchanges it invokes with CCMS.	Yes
Target (or Target Alias)	Unique identifier for the target system. The AOC will provide this unique value to all integration partners. For data exchanges inbound to CCMS this will be the unique value assigned to the CCMS system and will be used for all inbound data exchanges.	Yes
Interface Name	Identifier for the data exchange. Every data exchange name includes an identifier as part of the name. See "Appendix A—Data Exchange Names and Identifiers" for the list of data exchanges initiated by the integration partner, along with the associated identifier value.	Yes
Document Type	Identifier for the data exchange that helps uniquely identify an exchange and interface name. See "Appendix A—Data Exchange Names and Identifiers" for the list of data exchanges initiated by the integration partner, along with the associated identifier value.	Yes

Element Name	Description	Required
Document ID	Not used	No
Correlation ID	Unique message identifier provided by the source to enable correlation of response with requests in asynchronous data exchanges. [2]	Yes
Distribution ID	Internal ISB use	No
ISB Transaction ID	Unique identifier assigned by the ISB to a particular request. All invocations and activities of a data exchange within the ISB are tracked using this identifier. Integration partners can use the default value of minus one (-1). Use of this default CONSTANT value is an indicator an ISB Transaction ID must be created by the ISB upon receipt of the message from the integration partner. The generated ISB Transaction ID will be returned to the integration partner system as part of the acknowledgement (ACK) message sent back to the integration partner system.	Yes
Environment	Identifier for the environment where the data exchange is deployed. The current domain of values and associated environments are: • DEV (Development) • TST (Testing) • STG (Staging) • PRD (Production)	Yes
Hostname	Identifier for the machine name from where the data exchange originated.	Yes
Timestamp	Indicates the time when the message is sent from a system. XML schema 'dateTime' datatype - based on ISO extended format CCYY-MM-DDThh:mm:ss E.g., 2009-12-14T18:05:29.89-08:00	Yes

[2] Correlation ID is mandatory for all asynchronous exchanges except for EFL902- Send Clerk Review Notification. Please refer to section 3.4.1.2 for more details.

Element Name	Description	Required
Court CD	Unique identifier for an individual court, either text or number, that identifies the court which sends/receives the data exchange message. Although optional in the schema, this data element is required for all data exchanges. If the integration partner does not provide the Court CD of the destination court in the inbound message, the message will be rejected and error code (950000) is sent back to the partner. The inbound message could be the inbound request or inbound response from the partner. See "Appendix B—Code Values for the Court CD ISB Schema Element" for allowable values.	Yes
User ID	Identifier for the user or system that originated the data exchange	No
Routing Info	Content-based routing information that is interpreted by the routing service to send the data exchange message to one or more integration partners. **Note**: This is only used for data exchanges outbound from the CCMS system. At this time, it is not applicable for integration partner use.	No
Sequencing Info/Id	Allows an integration partner to specify an order/sequence for processing of a set of data exchanges bound for the court. Sequencing Info elements contain information required to ensure that the ISB delivers messages to the target system in sequential order. The ID element indicates the sequence number for a message as related to a specific interface.	No
Sequencing Info/RelatedSequenceID	RelatedSequenceID field indicates sequence as related to last message processed by the ISB for a specific interface. This must be provided by the source system.	No
Sequencing Info/GroupId	Group ID's represent a logical block of messages that need sequencing. This must be provided by the source system.	No

3.4.1.4 ISB Additional Parameter Settings schema

The ISB provides a schema named "Additional Parameters" that is used when custom ISB settings are required instead of the default ISB message delivery settings, and can be used to override two specific default settings:

- Retry/Replay settings
- Message Sequencing settings

The ISB Additional Parameters schema is located in the "ISBAdditionalParams.xsd" schema file.

Note: For data exchanges inbound to the court, the CCMS and ISB systems may use the additional parameter contents supplied by the integration partner system. For data exchanges outbound from the court, the additional parameter schema elements are not relevant for the integration partner system and can be ignored.

3.4.1.5 Retry/Replay settings

The role of the Retry/Replay service on the ISB is to insure, where possible, reliable delivery of the message to the target system. The inbound data exchanges currently using the Retry/Replay service are all configured to use the default setting. The default Retry/Replay setting will attempt to retransmit the message to the CCMS system every 10 minutes up to three times, before being declared unsuccessful and returning an error to the source (integration partner) system. If custom settings are required by the integration partner for a data exchange, Table 2 lists the elements along with their definitions.

Note: Integration partners must contact the AOC Data Integration group before applying custom Retry/Replay settings to any inbound data exchange so that the full impact of the settings can be evaluated and validated in advance.

Table 2. Retry/Replay Settings Element Names

Element Name	Description	Required
TTL	Duration for which the message will be retained in the ISB (in milliseconds.)	No
Destination	ISB specific information required for replay processing. The AOC will provide integration partners with the appropriate destination values as needed.	No
Max Replay Count	Number of replay attempts automatically performed by the ISB in its attempt to transfer the message to the target system (CCMS.)	No
Replay Schedule	Time interval between replay attempts (hours/minutes/seconds.)	No
Cut Off Schedule	Time interval (after initially receiving the message) during which the ISB will automatically attempt to replay the message (hours/minutes/seconds.)	No

3.4.1.6 CCMS Exchange Sequencing settings

An integration partner may need to set the order in which data exchange messages are processed by the CCMS system.

For example, an integration partner could submit exchanges for arrest notification and for bail notification. In this case, the integration partner would want the arrest notification processed ahead of the bail notification.

To do this, the integration partner must perform the following steps:

1. Retrieve the value of the ISB Transaction ID from the acknowledgement message received for the arrest notification exchange.
2. For the subsequent bail notification exchange, edit the “NVPairs” complex type elements located in the Additional Parameters schema.
3. Include “DEPENDANT_TRANSACTION_ID” in the “Name” element.
4. Include the ISB Transaction ID obtained from the arrest notification exchange in the “Value” element.
5. Submit the bail notification exchange.

Table 3 lists the CCMS exchange sequencing settings element names.

Table 3. CCMS Exchange Sequencing Settings Element Names

Element Name	Description	Required
Name	This must contain the following literal “DEPENDANT_TRANSACTION_ID”	No
Value	Value of the ISB Transaction ID for the exchange on which this exchange is dependent.	No

When the CCMS system attempts to process the bail notification exchange and discovers the ISB Transaction ID in the additional parameters area it will verify that the exchange associated with the ISB Transaction ID (arrest notification) is processed ahead of the bail notification exchange.

3.4.1.7 Common Response Message schema

This is used as a synchronous technical acknowledgement (ACK) in output schema for all asynchronous data exchanges. This is used to indicate the successful receipt of message by the ISB, either from the integration partner or CCMS. This is not a functional response message. From an integration partner perspective, depending on the specific data exchange this message may be followed by a functional success or error message from the associated application in CCMS. This Common Response Message is located in the "ISBCommonServiceResponseSchema.xsd" schema file.

Note: Integration partners will never populate the Common Response Message. It is only populated by the ISB. An integration partner will only receive a Common Response Message from the ISB as a technical acknowledgement (ACK) for receipt of an asynchronous data exchange. Table 4 lists the common response message schema element names.

Table 4. Common Response Message Schema Element Names

Element Name	Description	Required
Status	Contains the status associated to the data exchange response (i.e., success or failure.)	Yes
Message	Contains a free-form message to provide additional status information in the data exchange response	Yes
Document ID	Identifier for the individual message. The target system provides the same value that was present in the original request received by the target system.	No
Correlation ID	Identifier for the individual message used for correlating response(s) for target system(s). The source system provides the value.[3]	Yes
Sequence ID	Identifies the unique message within a batch or group of messages	No
ISB Transaction ID	Unique identifier assigned by the ISB to a particular request. All invocations and activities of a data exchange within the ISB are tracked using this identifier.	Yes
Timestamp	Indicates the time when the message is sent from a system.	Yes

3.4.1.8 Common Error Message

This is used synchronously when an error condition is encountered on the ISB prior to the target system receiving the message. From the perspective of an integration partner, this error condition

[3]Correlation ID is mandatory for all asynchronous exchanges except for EFL902- Send Clerk Review Notification. Please refer to section 3.4.1.2 for more details.

message will be populated by the ISB and will only be triggered when a message from integration partner inbound to the court generates the error. These error type conditions include schema validation errors, errors related to routing and system unavailable errors. These are not functional type errors generated by the court application on the CCMS system. This ISB Common Error Message is located in the "ISBCommonErrorSchema.xsd" schema file.

Note:

- Integration partners will never populate the Common Error Message, which is only populated by the ISB.
- For asynchronous data exchanges, the integration partner's request will receive either a "Common Error Message" or a "Common Response Message."
- Integration partners will require a notification service in order to receive Common Error Messages generated by the ISB following the Common Response Message acknowledgement (see Figure 2.)

Table 5 lists the common error message element names.

Table 5. Common Error Message Element Names

Element Name	Description	Required
Exception Code	Contains the error code associated to a data exchange response (i.e., success or failure)	Yes
Exception Message	Contains free form message to provide additional error information in the data exchange response	No
Exception Details	Technical details such as stack trace of the exception that occurred in the date exchange process in the ISB.	No

3.4.1.9 Global Notification

The Global Notification allows integration partners to receive notification from ISB. In an asynchronous data exchange, partners send their request and wait for CCMS system to process the request. There are few steps involved before CCMS starts processing the request, such as ISB performing payload validation, data transformation and forwarding the request to CCMS. The request may fail during any of these steps. Global Notification service allows partners to receive the status of their request during these steps.

The notification can be a success (Confirmation Channel) or error message (Exception Channel).

Note: Integration partners should develop and maintain a notification service to consume this notification.

3.4.1.9.1 Confirmation Channel

This is used to indicate the successful transfer of data to CCMS. This is not a functional response message. From an integration partner perspective, depending on the specific data exchange this message may be followed by a functional success or error message from the associated

application in CCMS, as shown in Figure 2. The Confirmation Channel Service Message is located in the “ConfirmationChannelService.xsd” schema file. The structure of Confirmation Channel Service is shown in Figure 3.

Note: Integration partners will never populate the Confirmation Channel Message. It is only populated by the ISB. An integration partner will only receive a Confirmation Channel Message from the ISB.

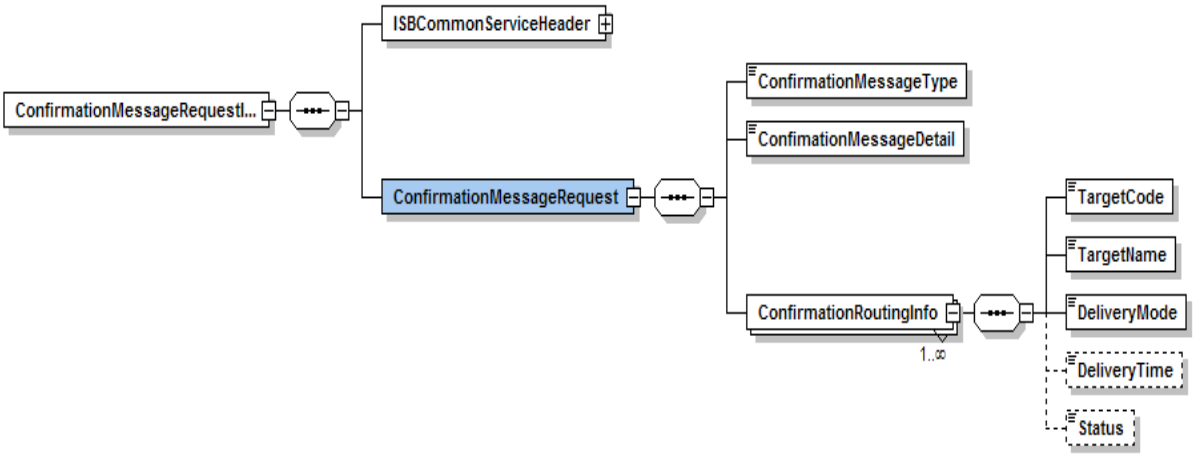

Figure 3. Confirmation Channel Schema Structure

Table 6 lists the confirmation channel message schema element names.

Table 6. Confirmation Channel Message Schema Element Names

Field Name	Required	Description
ConfirmationMessageType	Y	Confirmation Message Type for e.g. CBR
ConfirmationMessageDetail	Y	Confirmation Message Detail
ConfirmationRoutingInfo	Y	These elements provide information related to content based routing.
ConfirmationRoutingInfo/TargetCode	Y	Target code i.e. alias of target system
ConfirmationRoutingInfo/TargetName	Y	Target name i.e. detailed name of target system
ConfirmationRoutingInfo/DeliveryMode	Y	Delivery mode i.e. what type of transport used or will be used to deliver the message to specific target system
ConfirmationRoutingInfo/DeliveryTime	N	Message delivery time i.e. when the message was delivered
ConfirmationRoutingInfo/Status	N	Status of message i.e. Ready for delivery or Delivered

3.4.1.9.2 Global Exception Channel

This is used asynchronously when an error condition is encountered on the ISB prior to the target system (CCMS) receiving the message. From the perspective of an integration partner, this error condition message will be populated by the ISB and will only be triggered when a message from integration partner inbound to the court generates the error. These error type conditions include schema validation errors, errors related to routing, and system unavailable errors. These are not functional type errors generated by the court application on the CCMS system, as shown in Figure 2. This Exception Channel Error Message is located in the "ExceptionChannelService.xsd" schema file. The structure of Exception Channel Service is shown in Figure 4.

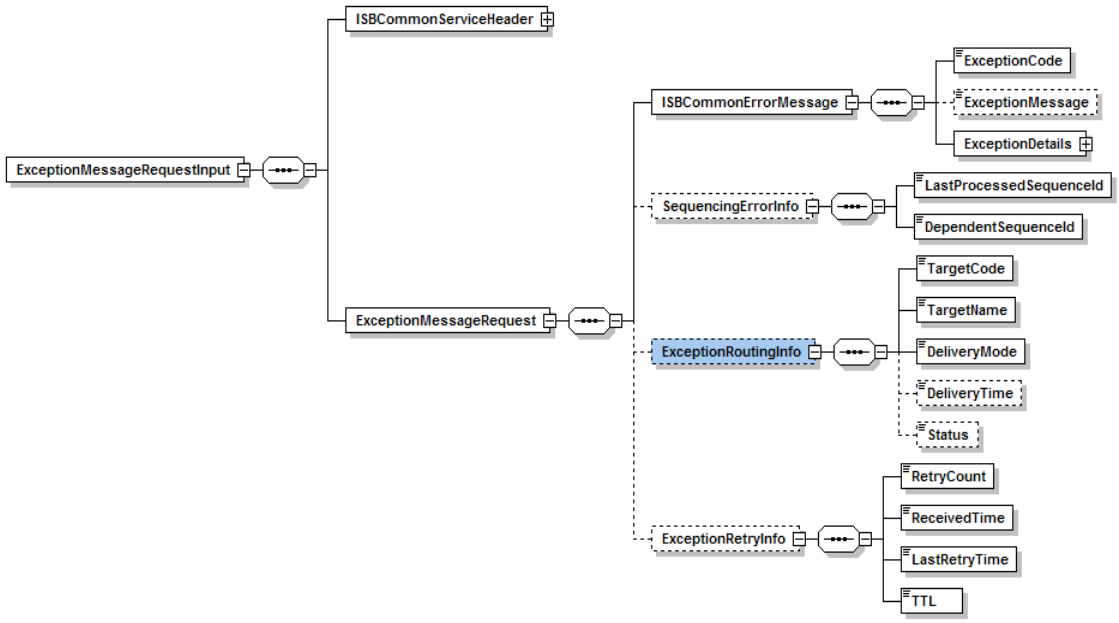

Figure 4. Exception Channel Schema Structure

Table 7 shows the exception channel message schema element names.

Table 7. Exception Channel Message Schema Element Names

Field Name	Required	Description
ISBCommonErrorMessage	Y	Error Details
ISBCommonErrorMessage/ExceptionCode	Y	Exception Code
ISBCommonErrorMessage/ExceptionMessage	N	User friendly error message i.e. description of error that can be shown to the users.
ISBCommonErrorMessage/ExceptionDetails	Y	Detailed error message (like stack trace) for troubleshooting purposes
ISBCommonErrorMessage/ExceptionDetails/Stack Trace	Y	Stack trace
ISBCommonErrorMessage/ExceptionDetails/Msg	Y	Message
ISBCommonErrorMessage/ExceptionDetails/FullCl ass	Y	Full class name
ISBCommonErrorMessage/ExceptionDetails/Class	Y	Class name
ISBCommonErrorMessage/ExceptionDetails/Data	N	Data or additional information
SequencingErrorInfo	N	Sequencing related error details
SequencingErrorInfo/LastProcessedSequenceId	Y	Last Processed Sequence Id
SequencingErrorInfo/DependentSequenceId	Y	Dependent Sequence Id
ExceptionRoutingInfo	N	These elements provide information related to content based routing.
ExceptionRoutingInfo/TargetCode	Y	Target code i.e. alias of target system
ExceptionRoutingInfo/TargetName	Y	Target name i.e. detailed name of target system
ExceptionRoutingInfo/DeliveryMode	Y	Delivery mode i.e. what type of transport used or will be used to deliver the message to specific target system
ExceptionRoutingInfo/DeliveryTime	N	Message delivery time i.e. when the message was delivered
ExceptionRoutingInfo/Status	N	Status of message i.e. Ready for delivery or Delivered
ExceptionRetryInfo	N	Retry details
ExceptionRetryInfo /RetryCount	Y	How many times retry attempt was made
ExceptionRetryInfo /ReceivedTime	Y	Received time
ExceptionRetryInfo /LastRetryTime	Y	Last Retry time
ExceptionRetryInfo /TTL	Y	Time to live information

Appendix A—Data Exchange Names and Identifiers

Table 8 contains the data exchange name and identifier for only those exchanges initiated by an integration partner and destined for the courts. This table excludes the data exchanges initiated by the court and destined for an integration partner. For the court-initiated exchanges, the "Interface Name" ISB header value will be populated by the CCMS system.

Table 8. Data Exchange Names and Identifiers

Data Exchange Name	Identifier
ACC801 Receive Victim Restitution Establishment Request	ACC801
ACC802 Receive Cash Bail Notification	ACC802
ACC803 Receive Bail Bond Notification	ACC803
APL802 Receive Order, Disposition Order, Opinion Notification (ACCMS)	APL802
APL803 Receive Remittitur Notification (ACCMS)	APL803
APP801 Receive Case Search Query	APP801
CAL801 Receive Calendar Event Request	CAL801
CAL803 Receive Court Resource Vacation Dates Notification	CAL803
CAL805 Receive Case Calendar Information Query	CAL805
CAS801 Receive Case Summary Query	CAS801
CAS806 Receive Public Defender Assignment Notification	CAS806
CAS807 Receive Case Notice List Query	CAS807
COL805 Receive Collections Franchise Tax Board (FTB) Case Return Notification	COL805
DOJ802 Receive Disposition Error Report Notification	DOJ802
DSP816 Receive Proposed Recommendation Filing (MOCS Codes)	DSP816
DSP821 Receive Probation Violations Update Notification	DSP821
DSP822 Receive Draft Minute Order Notification	DSP822
EFL801 Receive Accounting Reconciliation Report from EFSPs Notification	EFL801
EXB801 Receive Exhibits List Notification	EXB801

Data Exchange Name	Identifier
FCC801 Receive Traffic School Completion Notification	FCC801
FCC802 Receive Traffic School Extension Request	FCC802
FCC803 Receive Appearance Date Extension Request	FCC803
FCC804 Receive Traffic School Enrollment Request	FCC804
FCC806 Receive Payment Notification	FCC806
FCC807 Receive Case Participant Balance Query	FCC807
INI801 Receive Case Initiation Filing-– Citations	INI801
INI802 Receive Case Initiation Filing-- Felony, Misdemeanor and Infraction (FMI)	INI802
INI803 Receive Case Initiation Filing-– Juvenile	INI803
INI804 Receive Case Initiation Filing-- Small Claims	INI804
INI805 Receive Case Initiation Filing-- Civil Limited Unlimited	INI805
INI806 Receive Case Initiation Filing-- Family Law (Adoption)	INI806
INI807 Receive Case Initiation Filing-- Family Law (Marriage DP with without Child)	INI807
INI808 Receive Case Initiation Filing-- Family Law (CRPO)	INI808
INI809 Receive Case Initiation Filing-- Family Law (UIFSA)	INI809
INI810 Receive Case Initiation Filing-- Family Law (Petition for Custody Support)	INI810
INI811 Receive Case Initiation Filing-- Family Law (DVP with without Child)	INI811
INI812 Receive Case Initiation Filing-- Family Law (Registration of Judgment or Order)	INI812
INI813 Receive Case Initiation Filing-- Family Law (Miscellaneous)	INI813
INI814 Receive Case Initiation Filing-- No Complaint Filed (NCF)	INI814
INI815 Receive Employment Dev Dept (EDD) Case Upload	INI815
INI816 Receive Subsequent Case Filing	INI816
INI819 Receive Case Initiation Filing-- Mental Health	INI819
INI820 Receive Case Initiation Filing-– Probate	INI820

Data Exchange Name	Identifier
ISS802 Receive Warrant Status Update Notification	ISS802
ISS803 Receive Warrant Re-issuance Purge Request	ISS803
ISS804 Receive Warrant Proof of Service Notification	ISS804
ISS806 Receive Civil Issuances Query	ISS806
PF802 Receive Additional Demographic Information Notification	PF802
PF804 Receive Case Participant In-Custody Indicator Notification	PF804
PF805 Receive Attorney Details by Bar Number Query	PF805
PF806 Receive Attorney Details by Name Query	PF806
PF807 Receive Family Unit Update Request	PF807
PHX802 Receive Disbursement Update Notification	PHX802
PHX806 Receive Bad Check Notification	PHX806

Appendix B—Code Values for the Court CD ISB Schema Element

Table 9 contains the code values to be used for the "Court CD" ISB schema element.

Table 9. Code Values for the Court CD ISB Schema Element

County Court	Code	County Court	Code
Alameda	01	Alpine	02
Amador	03	Butte	04
Calaveras	05	Colusa	06
Contra Costa	07	Del Norte	08
El Dorado	09	Fresno	10
Glenn	11	Humboldt	12
Imperial	13	Inyo	14
Kern	15	Kings	16
Lake	17	Lessen	18
Los Angeles	19	Madera	20
Marin	21	Mariposa	22
Mendocino	23	Merced	24
Modoc	25	Mono	26
Monterey	27	Napa	28
Nevada	29	Orange	30
Placer	31	Plumas	32
Riverside	33	Sacramento	34
San Benito	35	San Bernardino	36
San Diego	37	San Francisco	38
San Joaquin	39	San Luis Obispo	40

County Court	Code	County Court	Code
San Mateo	41	Santa Barbara	42
Santa Clara	43	Santa Cruz	44
Shasta	45	Sierra	46
Siskiyou	47	Solano	48
Sonoma	49	Stanislaus	50
Sutter	51	Tehama	52
Trinity	53	Tulare	54
Tuolumne	55	Ventura	56
Yolo	57	Yuba	58

Appendix C—Username Token Header

Working SOAP Header UNT example:

```
<soapenv:Header>
<wsse:Security soapenv:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
         <wsse:UsernameToken>
            <wsse:Username>XXXXXXXXX</wsse:Username>
            <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">XXXXXXXXXX</wsse:Password>
            <!--wsu:Created xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2011-03-30T23:59:45.690Z</wsu:Created>
            <wsse:Nonce>W1N23IcrN/Xbz7CQW2YOGw==</wsse:Nonce-->
         </wsse:UsernameToken>
      </wsse:Security>
</soapenv:Header>
```

Working OWSM response policy:

```
<wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:oralgp="http://schemas.oracle.com/ws/2006/01/loggingpolicy"
xmlns="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="wss_username_token_service_policy"
xmlns:orasp="http://schemas.oracle.com/ws/2006/01/securitypolicy"
xmlns:orawsp="http://schemas.oracle.com/ws/2006/01/policy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <sp:SupportingTokens xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">
    <wsp:Policy>
      <sp:UsernameToken
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
        <wsp:Policy>
          <sp:WssUsernameToken10/>
        </wsp:Policy>
      </sp:UsernameToken>
    </wsp:Policy>
  </sp:SupportingTokens>
</wsp:Policy>
```