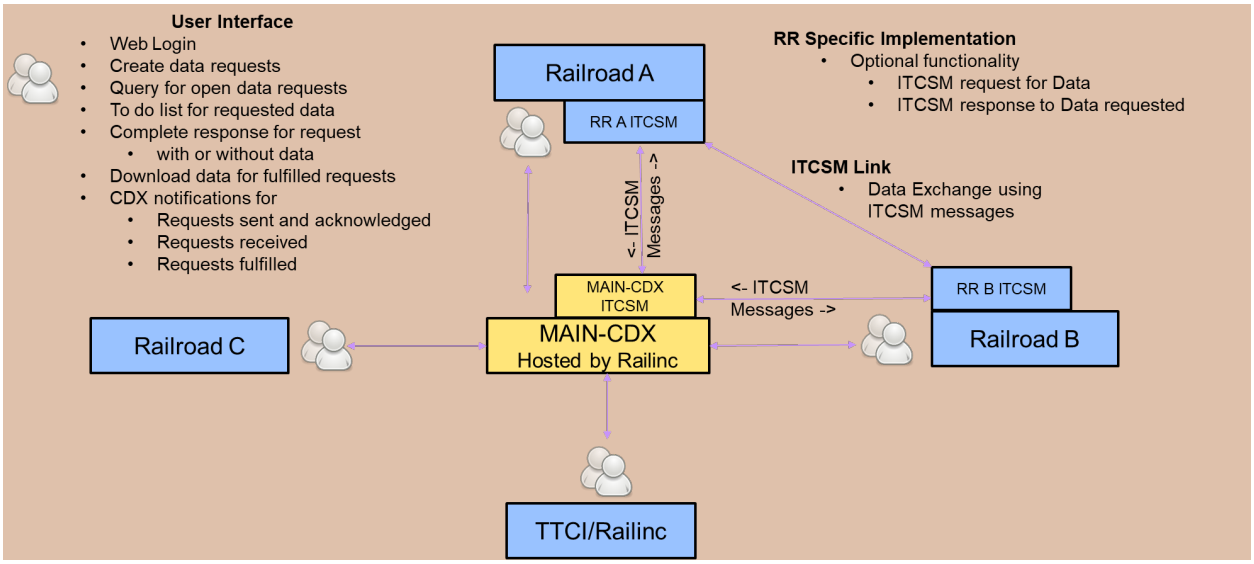
U.S. Department
of Transportation
Federal Railroad
Administration

Office of Research,
Development and Technology
Washington, DC 20590

Monitoring and Analysis of the Integrated Network (MAIN): Phase II Final Report



REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE:	3. DATES COVERED
26-03-2021	Technical Report	8/8/2018 – 7/5/2021

4. TITLE AND SUBTITLE
Monitoring and Analysis of the Integrated Network (MAIN): Phase II Final Report

5a. CONTRACT NUMBER
DTFR53-11-D-00008

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S):
Shad Pate – https://orcid.org/0000-0001-7191-5919
Mohamad Khater – https://orcid.org/0000-0002-1288-9906
Thomas Hall – https://orcid.org/0000-0001-5563-5335
Bryan Gillespie – https://orcid.org/0000-0002-1773-9931
Joseph Brosseau – https://orcid.org/0000-0002-2822-567X

5d. PROJECT NUMBER

5e. TASK NUMBER
693JJ618F000028

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Transportation Technology Center, Inc.
55500 DOT Road
Pueblo, Colorado 81001-4812

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT/FRA/ORD-21/22

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Railroad Policy and Development
Office of Research, Development, and Technology (RD&T)
Washington, DC 20590

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

13. SUPPLEMENTARY NOTES
COR: Jared Withers

14. ABSTRACT

Transportation Technology Center, Inc. (TTCI) developed, tested, and implemented a tool to support Interoperable Train Control (ITC)-compliant Positive Train Control (PTC) monitoring and troubleshooting. The tool, called the Monitoring and Analysis of the Integrated Network (MAIN)-Core Data Exchange (CDX), was developed by Railinc under the guidance of TTCI and an advisory group (AG) consisting of Class I railroads, shortline railroads, passenger and commuter railroads, FRA, and ITC-PTC vendors. MAIN-CDX is a web application, hosted by Railinc, with a user interface providing a standard method of requesting ITC-PTC asset data from other railroads, replying to requests received for asset data, and tracking of request status through a dashboard. The MAIN-CDX application was also integrated with railroad back offices over Interoperable Train Control System Management (ITCSM) messages to support the capabilities of creating data requests and responses through ITCSM messages rather than the user interface. MAIN-CDX has been well-received by the industry and is being used by railroads running ITC-PTC.

15. SUBJECT TERMS
ITC-PTC, PTC, ITC-PTC asset data, ITCSM, ITC-PTC monitoring, ITC-PTC troubleshooting, MAIN, MAIN-CDX

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Shad Pate, Principal Investigator, TTCI
Unclassified	Unclassified	Unclassified	Unclassified	64	19b. TELEPHONE NUMBER *(Include area code)* 719-584-7116

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXIMATE)

1 inch (in)	=	2.5 centimeters (cm)
1 foot (ft)	=	30 centimeters (cm)
1 yard (yd)	=	0.9 meter (m)
1 mile (mi)	=	1.6 kilometers (km)

AREA (APPROXIMATE)

1 square inch (sq in, in^2)	=	6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2)	=	0.09 square meter (m^2)
1 square yard (sq yd, yd^2)	=	0.8 square meter (m^2)
1 square mile (sq mi, mi^2)	=	2.6 square kilometers (km^2)
1 acre = 0.4 hectare (he)	=	4,000 square meters (m^2)

MASS - WEIGHT (APPROXIMATE)

1 ounce (oz)	=	28 grams (gm)
1 pound (lb)	=	0.45 kilogram (kg)
1 short ton = 2,000 pounds (lb)	=	0.9 tonne (t)

VOLUME (APPROXIMATE)

1 teaspoon (tsp)	=	5 milliliters (ml)
1 tablespoon (tbsp)	=	15 milliliters (ml)
1 fluid ounce (fl oz)	=	30 milliliters (ml)
1 cup (c)	=	0.24 liter (l)
1 pint (pt)	=	0.47 liter (l)
1 quart (qt)	=	0.96 liter (l)
1 gallon (gal)	=	3.8 liters (l)
1 cubic foot (cu ft, ft^3)	=	0.03 cubic meter (m^3)
1 cubic yard (cu yd, yd^3)	=	0.76 cubic meter (m^3)

TEMPERATURE (EXACT)

[(x-32)(5/9)] °F = y °C

METRIC TO ENGLISH

LENGTH (APPROXIMATE)

1 millimeter (mm)	=	0.04 inch (in)
1 centimeter (cm)	=	0.4 inch (in)
1 meter (m)	=	3.3 feet (ft)
1 meter (m)	=	1.1 yards (yd)
1 kilometer (km)	=	0.6 mile (mi)

AREA (APPROXIMATE)

1 square centimeter (cm^2)	=	0.16 square inch (sq in, in^2)
1 square meter (m^2)	=	1.2 square yards (sq yd, yd^2)
1 square kilometer (km^2)	=	0.4 square mile (sq mi, mi^2)
10,000 square meters (m^2)	=	1 hectare (ha) = 2.5 acres

MASS - WEIGHT (APPROXIMATE)

1 gram (gm)	=	0.036 ounce (oz)
1 kilogram (kg)	=	2.2 pounds (lb)
1 tonne (t)	=	1,000 kilograms (kg)
	=	1.1 short tons

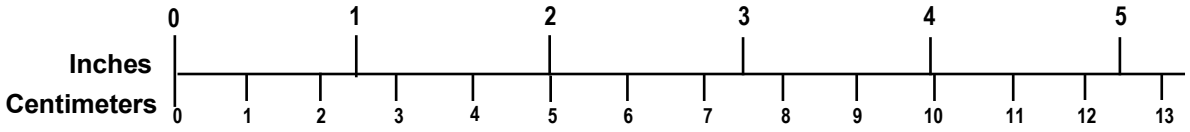
VOLUME (APPROXIMATE)

1 milliliter (ml)	=	0.03 fluid ounce (fl oz)
1 liter (l)	=	2.1 pints (pt)
1 liter (l)	=	1.06 quarts (qt)
1 liter (l)	=	0.26 gallon (gal)
1 cubic meter (m^3)	=	36 cubic feet (cu ft, ft^3)
1 cubic meter (m^3)	=	1.3 cubic yards (cu yd, yd^3)

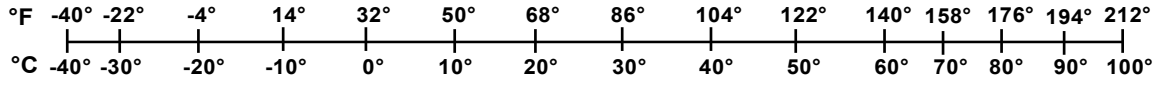
TEMPERATURE (EXACT)

[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSIO



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50 SD Catalog No. C13 10286

Updated 6/17/98

Acknowledgements

Transportation Technology Center, Inc. would like to acknowledge the following:

- The members of the advisory group for their technical guidance during the project, for providing input and feedback throughout the development of new Interoperable Train Control System Management (ITCSM) messages and requirements for data transfer operations between auto and manual railroads, and for participating in the user acceptance testing of the Monitoring and Analysis of the Integrated Network-Core Data Exchange (MAIN-CDX) application.
- Railinc for its efforts in the development of and user training for the MAIN-CDX application, incorporating the new ITCSM messages, and providing updated usage metrics for the MAIN-CDX application.
- The ITCSM working group and Meteorcomm LLC for supporting the requirements, creation, and implementation of the new ITCSM messages as well as for providing guidance and support throughout the integration process for the ITCSM messages between railroads and the MAIN-CDX application.

Table of Contents

Executive Summary viii
1. Introduction 1
1.1 Background 1
1.2 Objectives 2
1.3 Overall Approach 2
1.4 Scope 3
1.5 Organization of the Report 3
2. Project Overview 4
2.1 MAIN-CDX Data Requests and Responses 4
2.2 Overview of MAIN-CDX User Interface 5
2.3 Usage Metrics to Date 12
2.4 ITCSM Messages for MAIN-CDX 12
2.5 Data Transfer Use Cases and Message Flows 19
2.6 Data Format 23
2.7 Enhanced Monitoring and Troubleshooting of Foreign Locomotives 24
3. Conclusion 25
4. References 26
Appendix A: Proposed ITCSM Data Transfer, Data Response, and Notification Messages Version 0.20 27
Abbreviations and Acronyms 57

Illustrations

Figure 1. MAIN-CDX - Overview Diagram 5
Figure 2. Dashboard Table with Requests Example 1 (shows first seven columns)..... 7
Figure 3. Dashboard Table with Requests Example 2 (shows remaining columns)..... 8
Figure 4. Dashboard Advanced Search 8
Figure 5. MAIN-CDX Request Message Fields 9
Figure 6. Request Received and Request Status Options..... 10
Figure 7. Response Codes for Requested Assets 11
Figure 8. Uploading Logs with Response Code Complete for Requested Asset/Component ... 12
Figure 9. Message Flow Overview for Manual-to-Auto Request/Response..... 20
Figure 10. MAIN-CDX Request Fields used for the 10303 Data Transfer Request Message..... 21
Figure 11. Message Flow Overview for Auto-to-Manual Request/Response..... 22

Tables

Table 1. ITCSM Message Structure for 10303, 10304, 10305, and 10306 Messages 14
Table 2. 10303 Request Message Key Fields 15
Table 3. 10304 Response Message Key Fields 16
Table 4. 10305 Notification Message Key Fields 18
Table 5. 10306 Notification Response Message Key Fields 19

Executive Summary

Transportation Technology Center, Inc. (TTCI) conducted research, supported by the Federal Railroad Administration (FRA), to develop a tool railroads can use to monitor, troubleshoot, and analyze Interoperable Train Control (ITC)-compliant Positive Train Control (PTC) systems. This work was performed August 2018 to July 2021.

Called the Monitoring and Analysis of the Integrated Network-Core Data Exchange (MAIN-CDX), this tool was developed by Railinc under the guidance of TTCI and an advisory group (AG) consisting of Class I railroads, shortline railroads, passenger and commuter railroads, FRA, and ITC-PTC vendors. MAIN-CDX is a web application hosted by Railinc with a user interface that uses a dashboard to provide a standard method for requesting ITC-PTC asset data from other railroads, replying to requests received for asset data, and the tracking of request status. TTCI and Railinc collaborated with the AG to document the desired capabilities of the MAIN-CDX application. TTCI supported Railinc throughout the development and testing processes for the MAIN-CDX application. When first made available for use in December 2018, the MAIN-CDX provided users with the capability to manually create requests for ITC-PTC asset data, manually respond to requests for data, and view request status on a dashboard. As of the date of this report, the MAIN-CDX application has had 298 users across 54 railroads. These users have made over 23,400 data requests, with an average of approximately 1,300 requests generated per month over the 6 months prior to the writing of this report.

TTCI developed use cases that identified a need for four new ITC System Management (ITCSM) messages to support increased automation for creating and responding to requests for ITC-PTC data from other railroads. Interface requirements were developed and documented for the new ITCSM messages. Acceptance of the new ITCSM messages was provided by the AG, the ITCSM working group, and vendors implementing the System Management Gateways (SMGs) for ITCSM. TTCI supported Railinc with the implementation of the ITCSM messages in the MAIN-CDX application. TTCI also aided Railinc with defining the use cases for how the ITCSM messages will be used with the MAIN-CDX application to allow data transfer requests and responses between railroads using the ITCSM messages and railroads using the MAIN-CDX application. The release of the MAIN-CDX application that has been integrated with the ITCSM messages and supports data transfer and requests manually or through the use of ITCSM messages has been in use by the railroads since December 2020.

1. Introduction

Transportation Technology Center, Inc. (TTCI) conducted a research project, supported by the Federal Railroad Administration (FRA), to develop a tool railroads can use for monitoring, troubleshooting, and analyzing their Interoperable Train Control (ITC)-compliant Positive Train Control (PTC) systems (hereafter referred to as ITC-PTC) in interoperable operations.

ITC-PTC is a system designed to enhance safety through the enforcement of movement authority limits and speed restrictions. Monitoring, troubleshooting, and analyzing ITC-PTC systems is essential for quickly identifying and addressing issues to help maintain the high availability needed to achieve the safety benefits of ITC-PTC without unnecessary operational impact. This project introduced Monitoring and Analysis of the Integrated Network Core Data Exchange (MAIN-CDX), a tool used to assist the railroad industry with monitoring, troubleshooting, and analyzing issues associated with interoperable ITC-PTC operations. MAIN-CDX is a web application, hosted by Railinc, that provides railroads with the ability to efficiently request and transfer data manually, as well as view request details on a dashboard. To support the increased automation of requesting and transferring data, MAIN-CDX was integrated with four new Interoperable Train Control System Management (ITCSM) messages that will allow railroads to create requests, transfer data, and track requests through the messages in lieu of manual entry through the MAIN-CDX application.

1.1 Background

ITC-PTC has been implemented in the U.S. to meet the requirements of the Rail Safety Improvement Act of 2008. PTC is an advanced form of train control designed to improve safety of rail transportation by mitigating:

- Train-to-train collisions
- Over-speed derailments
- Incursions into established work zone limits
- Movement of a train through a switch lined in the wrong position

The development and implementation of ITC-PTC was challenging due to the thousands of assets (fixed and mobile) that needed to be equipped and integrated over a short timeframe, the system's complexity, and its demanding performance requirements. Additionally, each railroad's trains and plant must interoperate with ITC-PTC systems at other railroads to create one seamless, nationwide network.

To achieve the intended safety benefits of ITC-PTC, the system must consistently maintain a high level of availability. Additionally, since ITC-PTC failures can result in slowing and/or stopping trains, it is critical to keep the system operational to avoid delays of and disruptions to the flow of the nation's railroad traffic.

ITC-PTC is a form of communications-based train control, and a degradation of the communications network can lead to reduced ITC-PTC functionality which can result in operational inefficiencies. Message traffic is often the most readily available source of data used to diagnose the problems and analyze the performance of a distributed system such as PTC. However, due to the inherent complexity of PTC, additional information, such as ITC-PTC

onboard data logs, ITC wayside interface unit logs, etc., is often necessary to diagnose system problems.

While PTC assets may have some built-in test capabilities, those are generally used for component-specific, self-test purposes as opposed to the identification or diagnosing of system-level problems. To efficiently identify and evaluate issues at the system level, a large amount of message traffic and other data needs to be analyzed collectively. There is additional complexity associated with dense urban areas where multiple railroads interoperate and sometimes share assets. Certain problems encountered in one railroad's ITC-PTC operations may be influenced by the presence of another railroad's trains and their associated ITC-PTC communications traffic.

When faults and failures occur in a system as complex as ITC-PTC, it can be very difficult and time-consuming to troubleshoot—especially when the symptoms are intermittent. Further, system redundancies (e.g., availability of multiple communications paths) can mask problems. Thus, efficient and standardized system monitoring and troubleshooting tools and methods are needed so that PTC system problems can be anticipated and prevented, or, if detected, quickly diagnosed and repaired before having a significant impact on safety and traffic flow.

This project introduced MAIN-CDX, a tool that assists and expands upon current industry efforts to monitor, troubleshoot, and analyze ITC-PTC systems in interoperable operations.

1.2 Objectives

For this phase of the MAIN project, the objectives were to:

- Provide railroads with an application to support data requests from ITC-PTC assets owned by other railroads, respond to said data requests, and track request details through a dashboard.
    - Identify input and output data needed to support application capabilities.
- Develop a method to integrate railroad back offices with the application to support automation of data requests and data transfers as well as assist with troubleshooting of shared PTC assets.

1.3 Overall Approach

TTCI conducted this project with assistance from an industry advisory group (AG). This AG consisted of representatives from FRA, Class I railroads, shortline railroads, passenger railroads, Railinc, and PTC vendors.

The overall approach included working with the AG to create the MAIN-CDX application that satisfied the railroads' needs for requesting data, transferring data, and tracking request statuses. To achieve this, TTCI first identified the input and output data needed for the MAIN-CDX application and the different use cases that MAIN-CDX needed to support. TTCI also defined the message specifications for four new ITCSM messages to be used with MAIN-CDX. These specifications were documented and will be provided to the Association of American Railroads (AAR) for incorporation into a future release of S-9460, the industry standard interface control document for ITCSM messages [1].

The MAIN-CDX application was created by and is housed at Railinc and is accessible by authorized railroad users through the web application or through railroads' PTC back offices using ITCSM messages. The MAIN-CDX web application was initially tested through railroad user acceptance testing (UAT) of manual data requests and responses before being released for manual railroad use. Additional UAT testing was completed for web application updates and for integration with ITCSM messages with the newest release of MAIN-CDX supporting manual railroad data requests and responses as well as automated requests and responses through the ITCSM messages.

1.4 Scope

MAIN Phase II supported the creation and evaluation of an industry standard MAIN tool called MAIN-CDX which has the capability to allow railroads to:

- Log in and manually create requests for data, respond to requests, and view the status of requests through the application dashboard.
- Send and receive ITCSM messages to create requests, respond to requests, and track request status using ITCSM messages in lieu of each railroad using the web application to create requests for data and respond to requests.

More specifically, the support included the development of documentation detailing the specifications of the new ITCSM messages needed to support MAIN capabilities and how the messages should integrate with MAIN-CDX. The documentation was provided to railroads, Railinc, and ITC-PTC vendors to assist with the implementation of the new ITCSM messages as well as with the integration between the railroad back offices and MAIN-CDX. The actual implementation and integration efforts were out of scope for the project, aside from consulting support.

The testing and analysis of the MAIN-CDX application was conducted over a series of UAT periods. TTCI provided Railinc with consulting support for the creation of Railinc's UAT test cases. TTCI also supported limited functionality testing of the MAIN-CDX application during UAT periods. Most UAT, and the ultimate acceptance of the application, was completed by participating railroads and Railinc with TTCI only providing consulting support. Railroads utilizing ITC-PTC operations involving one or more other railroads incorporated MAIN-CDX into back office systems to both use the application and provide feedback to TTCI and Railinc. TTCI provided consulting support to Railinc for reviewing user feedback and proposing updates to the application based on feedback. Usage of the MAIN-CDX application was monitored, and periodic metric updates, created by Railinc, were provided to the AG.

1.5 Organization of the Report

Section 2 of the report provides a project overview describing the capabilities of MAIN-CDX, the MAIN-CDX user interface, MAIN-CDX usage metrics, ITCSM messages used with MAIN-CDX, data format used within MAIN-CDX, and future considerations for monitoring and troubleshooting foreign locomotives. Section 3 provides a brief conclusion for this phase of the project. Appendix A includes the requirements defining the message structure, payload data, and message behavior for the four new ITCSM messages: 10303 Data Transfer Request Message, 10304 Data Transfer Response Message, 10305 Notification Message, and 10306 Notification Response Message.

2. Project Overview

When an ITC-PTC issue arises during interoperable operations, data from another railroad's ITC-PTC asset(s) are often required. Prior to MAIN-CDX, such an exchange of data was initiated by the host railroad requesting data from foreign ITC-PTC assets through phone calls or over e-mail. At times, that process resulted in significant delays in receiving the data, and, due to the informal nature of the request(s), in some cases, the data received was not what the requesting railroad required which resulted in additional e-mails or phone calls.

Interoperating railroads using ITC-PTC agreed that a standard tool was needed to request and transfer ITC-PTC data between one another. In collaboration with the AG and Railinc, TTCI supported the development and testing of the web application tool, MAIN-CDX. An overview of the capabilities of MAIN-CDX and ITCSM messaging developed under the MAIN Phase II project is provided in the following sections and includes:

- An overview of the MAIN-CDX data transfer methods (Section 2.1)
- An overview of the MAIN-CDX user interface (Section 2.2)
- The MAIN-CDX usage metrics (Section 2.3)
- An overview of the ITCSM messages developed for use with MAIN-CDX (Section 2.4)
- An in-depth look at the different data transfer methods (Section 2.5)
- An overview of the shared data format and future improvements (Section 2.6)
- A discussion of future options for improving the troubleshooting and monitoring of foreign locomotives (Section 2.7)

2.1 MAIN-CDX Data Requests and Responses

Data transfers between railroads can be carried out through a manual process using the MAIN-CDX application or through an automated (auto) process using ITCSM messages. Railroads that transfer data through auto ITCSM messages are referred to as "auto railroads," and railroads relying on manual requests are referred to as "manual railroads." The MAIN-CDX application supports data requests and responses from both manual and auto railroads—a high-level description of the data request and response use cases follows.

Manual-to-Manual requests/responses:

For data requests between two manual railroads, both the responding and requesting railroad use the MAIN-CDX application.

Auto-to-Manual requests/responses:

For a data request from an auto railroad to a manual railroad, the auto railroad sends an automated request to the MAIN-CDX application using an ITCSM message. MAIN-CDX parses the ITCSM message into a manual request within the MAIN-CDX application and notifies the manual railroad of the request. MAIN-CDX also replies to the auto railroad with an ITCSM response for the request. If the ITCSM response does not include the requested data, then the auto railroad periodically checks, through the use of ITCSM messages, with the MAIN-CDX application to see if data has been uploaded by the manual railroad.

Manual-to-Auto requests/responses:

For a data request from a manual railroad to an auto railroad, the manual railroad enters a request in the MAIN-CDX application. The MAIN-CDX application generates and sends the appropriate ITCSM messages to the auto railroad and provides the available data and request status to the manual railroad through the MAIN-CDX application.

Auto-to-Auto requests/responses:

For data requests between two auto railroads, the requesting railroad sends an ITCSM message directly to the responding railroad. The responding railroad uses ITCSM messages to respond to the requesting railroad. Once the requesting railroad receives a response, an ITCSM notification message is sent to the MAIN-CDX application to log and track the data transfer between the two auto railroads.

Figure 1 shows an overview diagram of MAIN-CDX, with Railroads A and B having both manual and auto capabilities and Railroad C being a manual railroad.

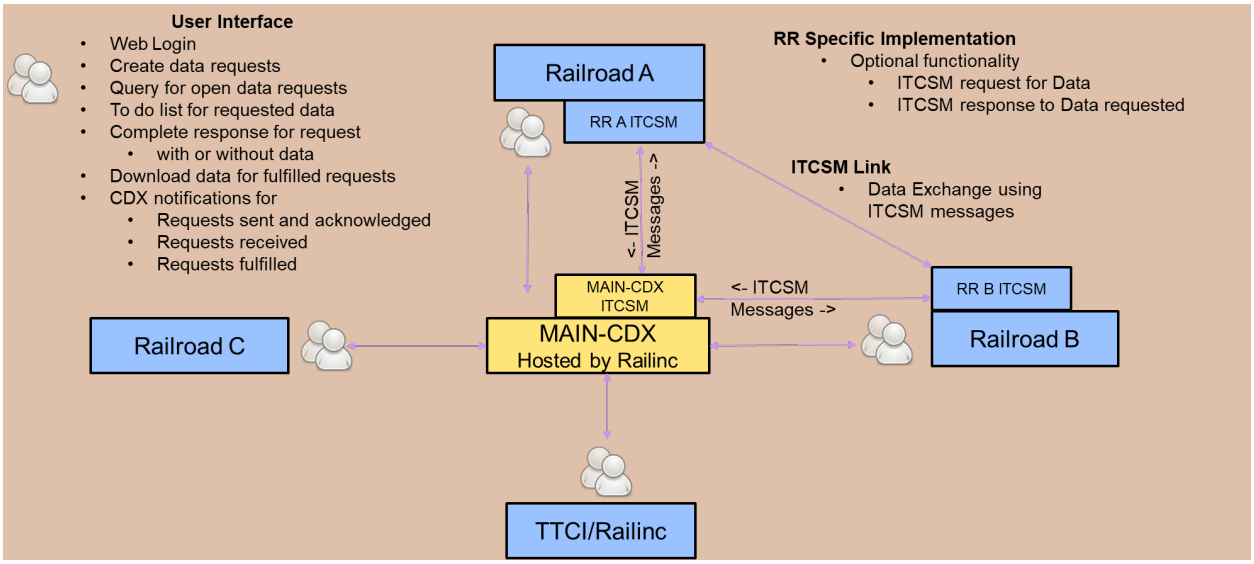


Figure 1. MAIN-CDX – Overview Diagram

2.2 Overview of MAIN-CDX User Interface

When data transfer messages are exchanged between two railroads and a manual railroad is involved, the MAIN-CDX application facilitates the creation of, sending of, and response to a request. When both end-users of the message transfer exchange are auto railroads, MAIN-CDX is not needed for the purpose of sending request or response messages. However, it is used to monitor requests created and the status of each request through notification messages sent by the auto requesting railroad. To support these needs, the user interface in the MAIN-CDX application includes a dashboard, a request page, and a response page.

2.2.1 Access to MAIN-CDX User Interface

Railroad users are granted access to the MAIN-CDX application by using Railinc's Single Sign-On (SSO) system. This system provides a common user registration process and a central repository for customer information, authentication, and authorization for Railinc's MAIN-CDX

application. If not already registered, a user must set up a user ID and password through Railinc's SSO. Once registered, the user must request access to the MAIN-CDX application, which includes selecting the user roles desired for the application. The request is reviewed by administrators from Railinc and the employing railroad before access is granted.

Users with access to the MAIN-CDX application can use the SSO to log in and launch the application. Users are only able to view and respond to requests for data that pertain to the railroad for which the user is authorized. Railroads are identified within MAIN-CDX by their Standard Carrier Alpha Code (SCAC). Similarly, users can only issue requests for data on behalf of the railroads for which they are authorized. Railroad SSO administrators are responsible for keeping authorized users up-to-date.

2.2.2 *MAIN-CDX User Interface Dashboard*

The dashboard is the main page in the MAIN-CDX application, and all requests can be viewed or accessed from this page. The functionality and data elements to include within the dashboard were identified with guidance from the AG. The dashboard only displays requests that pertain to the specific railroad user logged into the application. Information contained in the request fields, such as event type, request status, and requesting and responding railroads, is displayed in the dashboard columns as seen in Figure 2 and Figure 3. Dashboard table columns are listed below:

- Request ID: indicates the unique MAIN-CDX ID of each request.
- Event Type: indicates the event or category, such as "Initialization Error," "Braking Event," etc., for the assets that contain the logs if the request was initiated by a manual railroad; indicates the event type as "Automated Request" if the request was initiated by an automated railroad.
- Request RR: indicates the railroad that sent the request.
- Owning RR: indicates the railroad that owns the asset containing the requested logs.
- Requesting RR Ticket Ref ID: indicates the reference ID for the request, if provided.
- Asset Owning RR Ticket Ref ID: indicates the reference ID of the response, if provided.
- Event Date: indicates the date and time of the event.
- Asset ID: indicates the Edge Message Protocol (EMP) address or the System Management ID (SMID) of the asset requested along with the category of the asset, e.g., Locomotive, ITC Wayside Interface Unit, Other, etc.
- Create Date: indicates the date and time the request was created.
- Modified Date: indicates the date and time a change was made to the request.
- Status: indicates the request status, i.e., Submitted, Acknowledged, Responded, Completed, Cancelled, Denied.
- Request Direction: indicates if a request is Inbound (received by the user from another railroad) or Outbound (sent from the user to another railroad).

- Response Duration: indicates the duration between the time the request was created to the time the request status was changed to “Responded” as a result of having received a response.
- Data Purged: indicates if data has been purged.

The request fields displayed can be adjusted by selecting or unselecting the **Show/Hide columns** boxes. Searching for a specific request can be done by either entering the field details in any of the white search boxes, located under the table headings, or by using the dashboard advanced search function as seen in Figure 4.

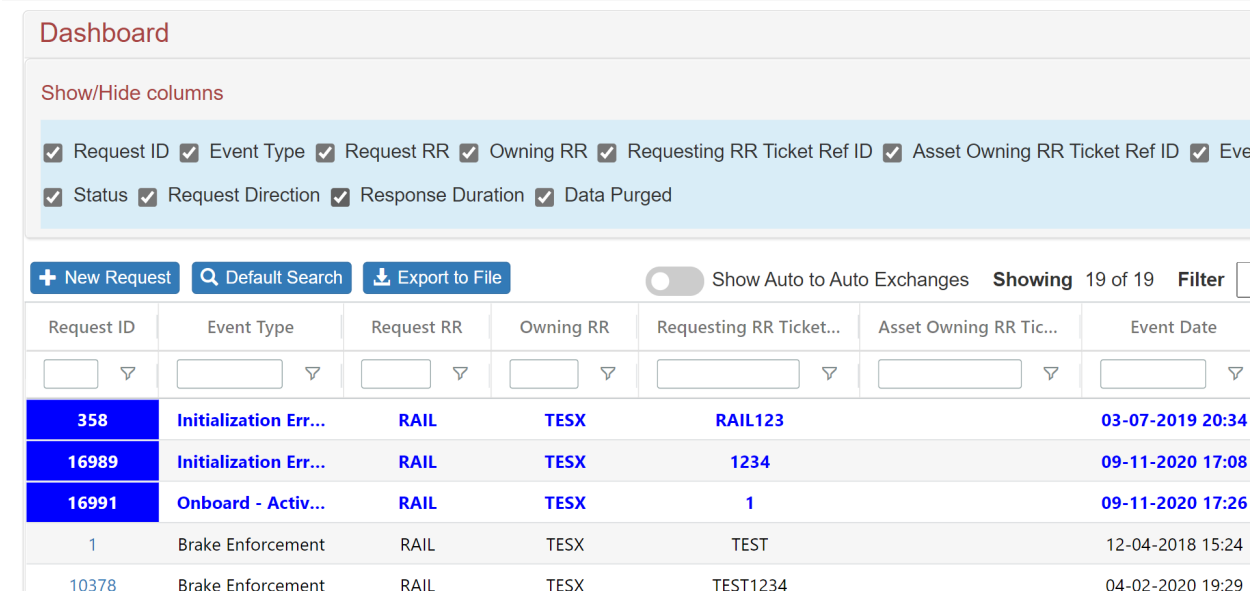


Figure 2. Dashboard Table with Requests Example 1 (shows first seven columns)

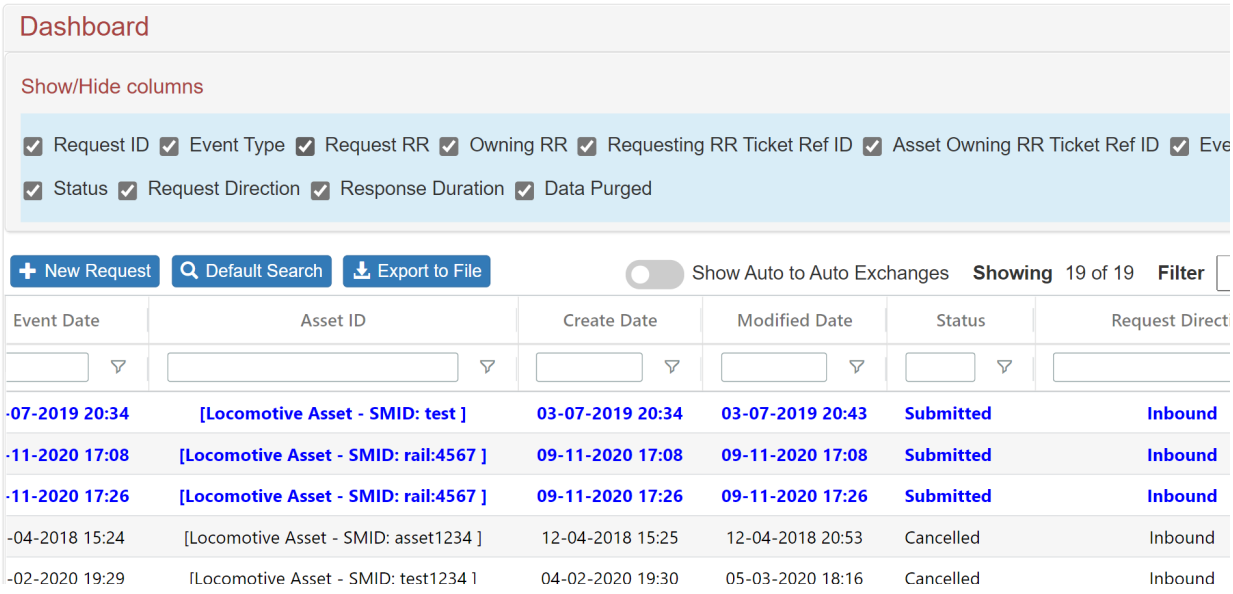


Figure 3. Dashboard Table with Requests Example 2 (shows remaining columns)

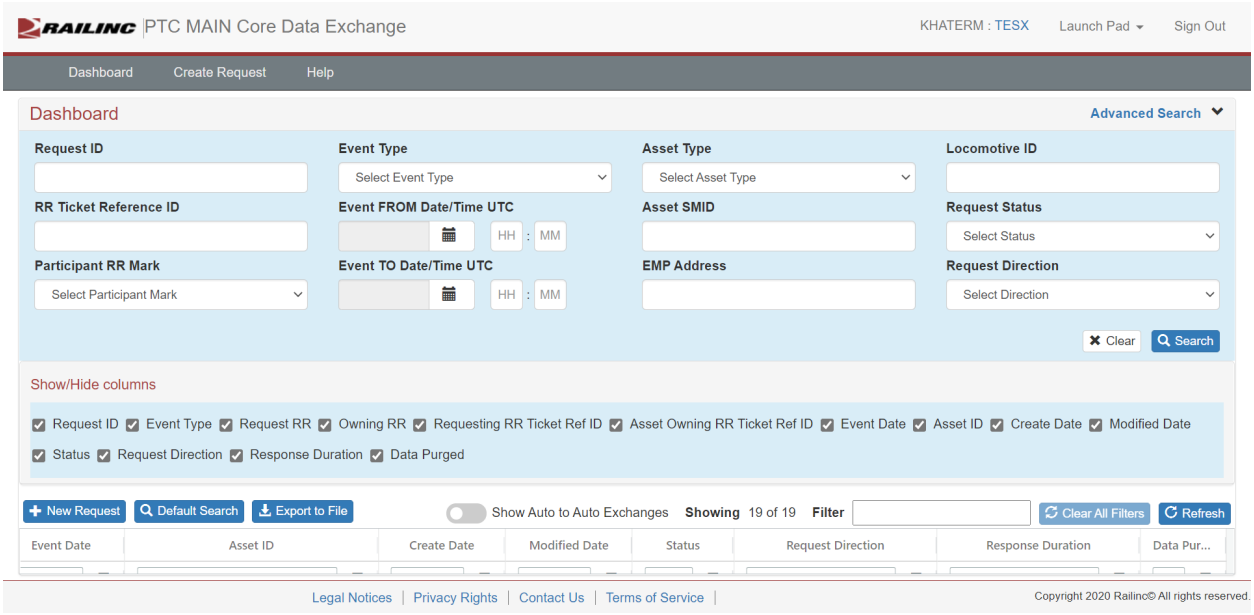


Figure 4. Dashboard Advanced Search

2.2.3 MAIN-CDX User Interface for Creating a Request

A new request message can be created either through the blue **New Request** box on the dashboard, shown in Figures 2–4, or by using the **Create Request** option found in the main bar of MAIN-CDX, shown in Figure 5. Input from the AG was used to determine the functionality and data needed to create a request for ITC-PTC data, which led to the design of the **New Request** page. To successfully create the request, all required fields of the request message must be populated. The request message fields in MAIN-CDX are shown in Figure 5, with required fields indicated by a red asterisk.

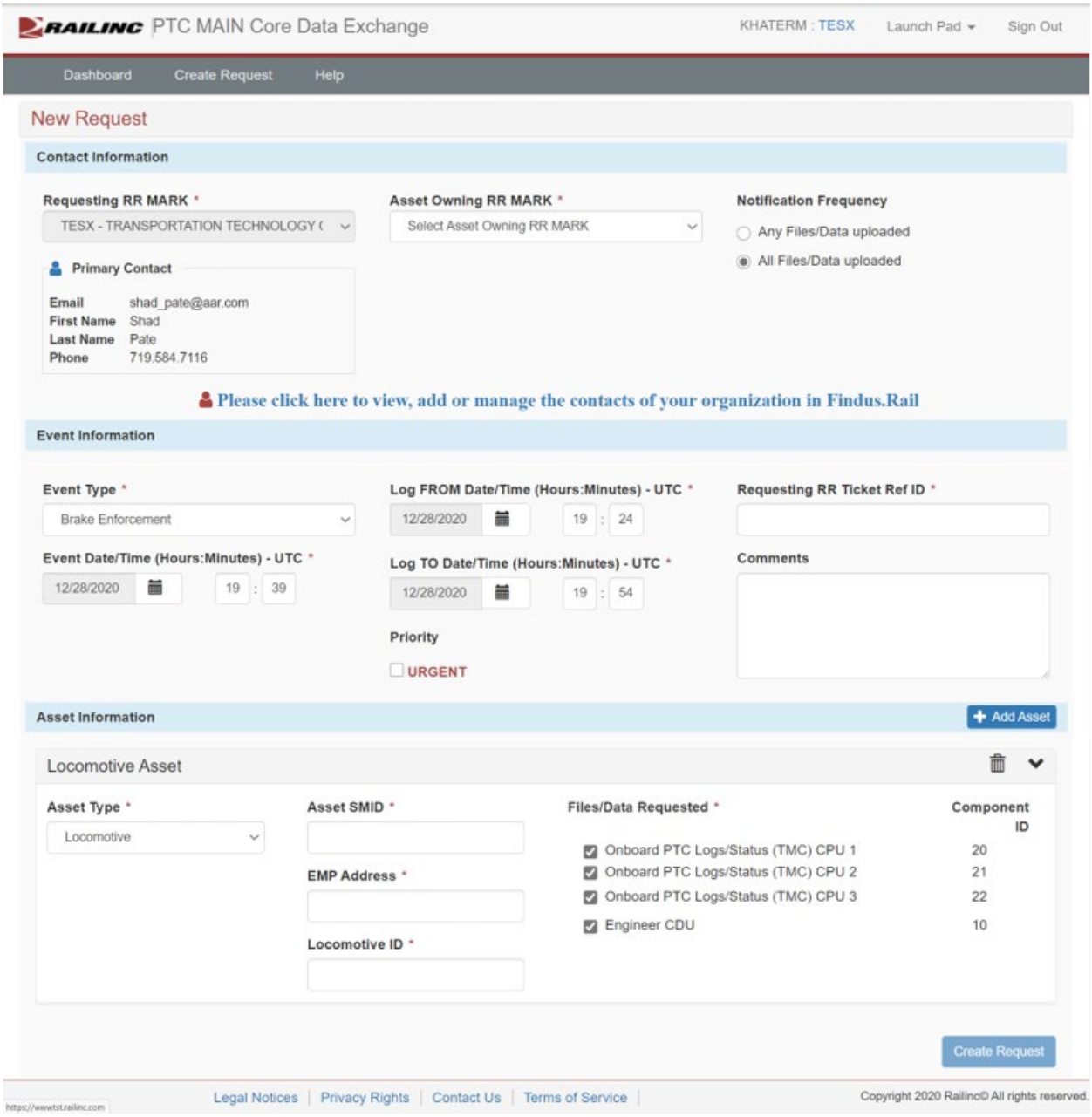


Figure 5. MAIN-CDX Request Message Fields

Once all required fields have been populated on the request page, the user can select the **Create Request** button, shown on the bottom-right corner of Figure 5, to create the request. If a request is sent to a manual railroad, a notification e-mail is sent to that railroad's MAIN-CDX users. If a request is sent to an auto railroad, data from the request will be used to create an ITCSM message that will be sent to the auto railroad.

2.2.4 MAIN-CDX User Interface for Responding to Request

Once a request is created, it is shown on both the requesting and the responding railroad's dashboard along with the information provided in the request fields. The request can be opened by selecting the request ID on the dashboard to view the logs requested from assets and

components. The responding railroad's MAIN-CDX users can perform different actions on the request, some that will generate notifications to the requesting railroad and some that will just update the status of the request on the dashboard. The following actions will either provide a notification to the requesting railroad or update the status in the dashboard:

- Denied: This status will notify the requesting railroad that the request was denied and update the request status on the dashboard.
- Submitted: This status will notify the requesting railroad that the request has been submitted, meaning the responding railroad has provided a response code for the request along with data, if available, and update the request on the dashboard.
- Acknowledged: This status will not provide a notification to the requesting railroad but will update the request status on the dashboard indicating that the responding railroad has viewed the request.
- Responded: This status will not provide a notification to the requesting railroad but will update the request status on the dashboard indicating that the responding railroad has acted on the request but has not yet submitted the response.

An example of a received request is shown in Figure 6, along with the "Request Status" update options that can be selected by the responding railroad user. The logs requested for each component can be uploaded, as shown in Figure 7. No further changes to the request are allowed when a response is in the Submitted state, but the responding railroad can revert the response status to Acknowledged and update the response if needed. If the response message contains logs, the logs can be downloaded by the requesting railroad, and the data will be purged from MAIN-CDX seven days after the response is submitted.

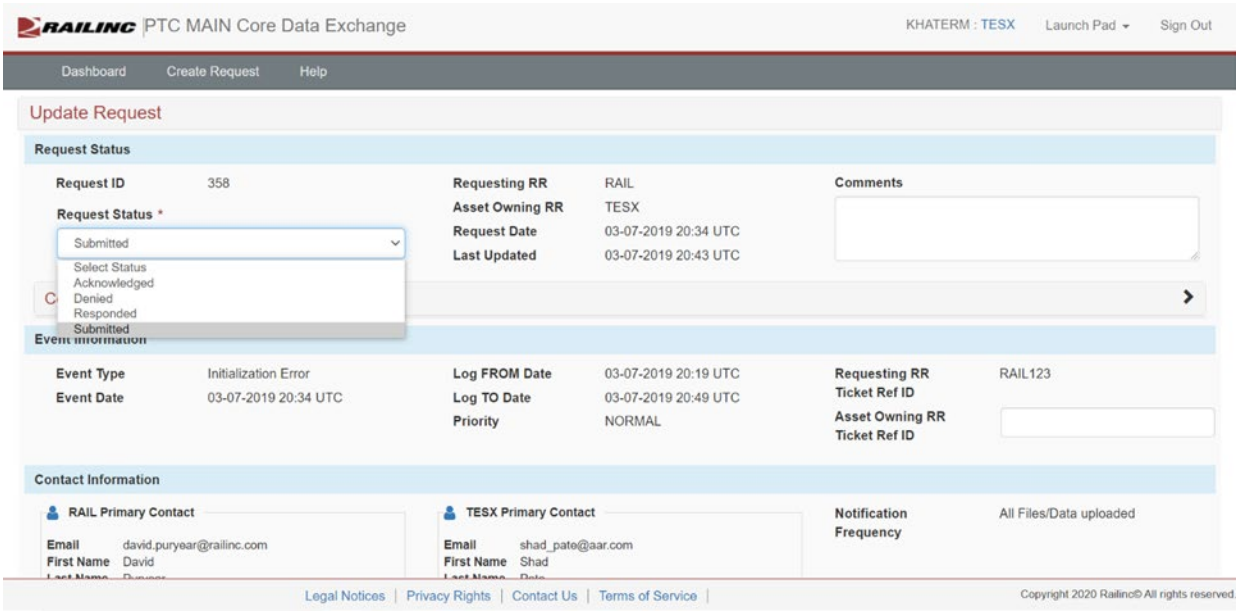


Figure 6. Request Received and Request Status Options

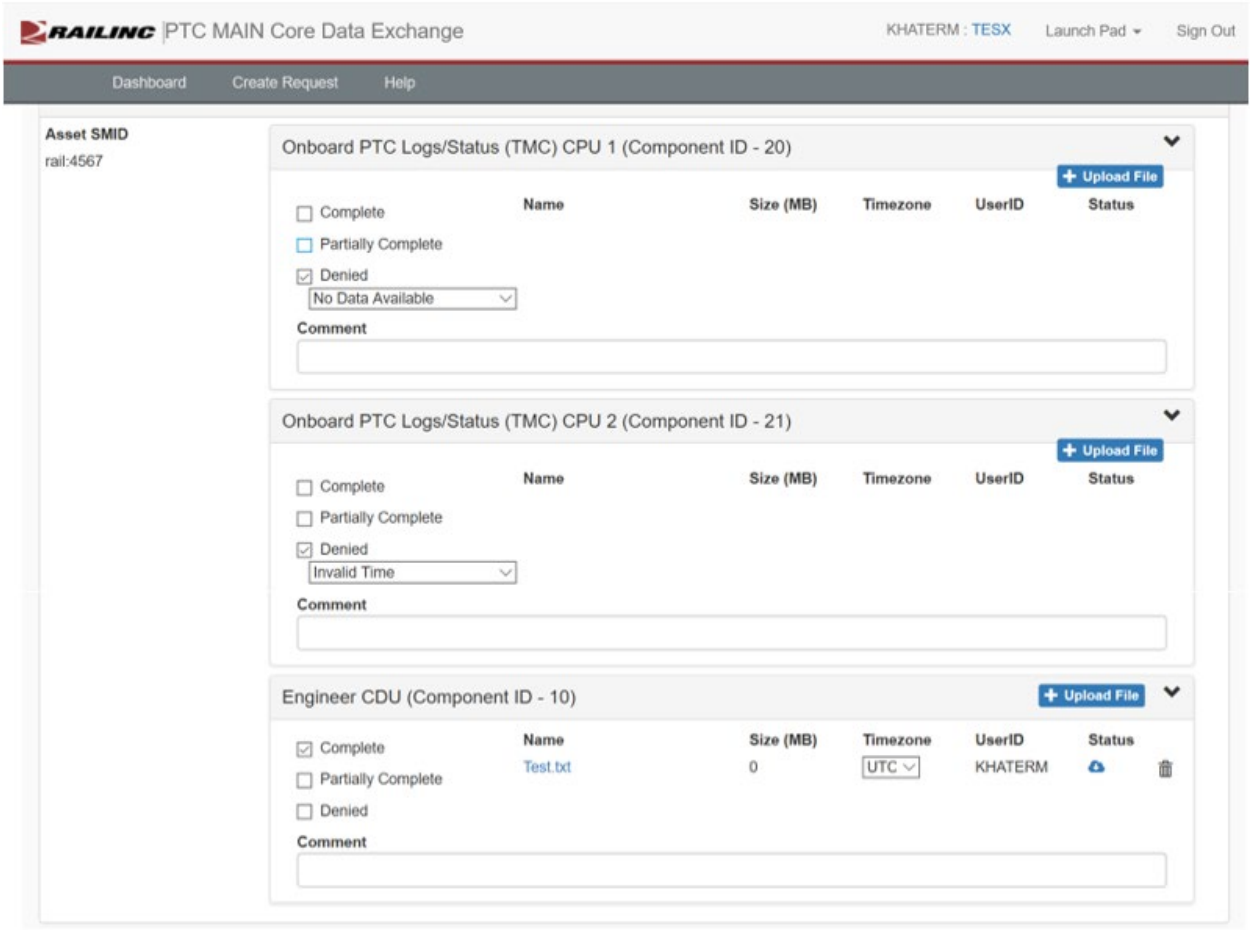


Figure 7. Response Codes for Requested Assets

2.2.5 MAIN-CDX User Interface for Downloading/Uploading Logs

When a request is received by MAIN-CDX, the asset owning railroad receives a notification. If the requested logs are available, the railroad uploads the logs using the blue **+ Upload File** box as seen in Figures 7 and 8. When a response message is received with the requested logs, the logs can be downloaded by clicking on the text file name.

Initially, when all data requests and responses were manual-to-manual through MAIN-CDX, railroads could upload multiple different files in multiple different file formats for a single request. Per AG guidance and interest in formalizing the data provided for requests to maintain consistency of responses from different railroads, the following requirements were defined:

- A response in the MAIN-CDX application is limited to a single text file for each asset component ID requested.
- The text file size must be less than 16 MB, as 16 MB is the maximum message size possible for a single EMP message used in the ITCSM messages integrated with MAIN-CDX.
- The text file must include the raw log data from the component requested.

As of the date of this report, the 16 MB size limit had not created any issues with data responses but could be increased in the future by modifying the ITCSM messages used for the data response to include fragmentation, which would allow multiple 16 MB EMP messages to be sent for a single request.

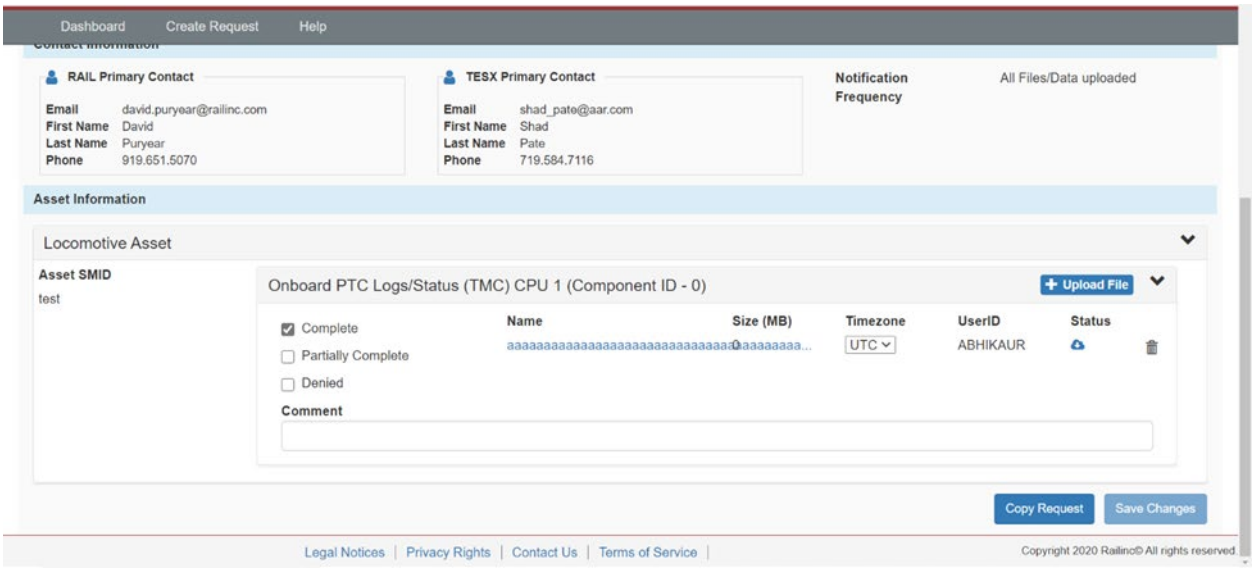


Figure 8. Uploading Logs with Response Code Complete for Requested Asset/Component

2.2.6 MAIN-CDX User Interface for Auto-to-Auto Transfers

When an auto-to-auto transfer occurs, notification messages are sent to MAIN-CDX to track the request status and the response messages involved. The notification messages can be seen by selecting the "Show Auto to Auto Exchanges" option located on top of the dashboard, as shown in Figure 2. The notification messages are sent by the auto railroad making the request, and, consequently, a notification response message is sent back from MAIN-CDX to acknowledge the reception of the notification message positively or negatively.

2.3 Usage Metrics to Date

MAIN-CDX is currently being used throughout the industry to share data for ITC-PTC issues in interoperable PTC operations. As of the date of this report, the MAIN-CDX application has had 298 users across 54 railroads. These users have made over 23,400 requests for data, with an average of approximately 1,300 requests generated per month over the 6 months prior to the writing of this report.

2.4 ITCSM Messages for MAIN-CDX

Initially, TTCI, the AG, and ITCSM working group members explored the use of existing ITCSM messages to integrate with MAIN-CDX. Ultimately, it was determined that the available messages were not adequate for creating messages to be used as data requests, data transfers, and notifications. Through the advisement of the AG and the ITCSM working group, TTCI developed documentation, provided in Appendix A, defining the requirements for four new ITCSM messages:

- Data Transfer Request Message, ITCSM message number 10303

- Data Transfer Response Message, ITCSM message number 10304
- Notification Message, ITCSM message number 10305
- Notification Response Message, ITCSM message number 10306

The documentation defines the requirements for each message with regard to the message structure, the payload data, and the desired behavior of the messages when used with MAIN-CDX. The document was reviewed and approved by the AG and the ITCSM working group and then supplied to the railroads and vendors planning to implement the messages with MAIN-CDX. The document defining the requirements for the four new ITCSM messages was submitted to AAR for inclusion in a future release of the AAR Manual of Standards and Recommended Practices (MSRP) as Standard S-9460, ITCSM Interface Control Document for Interoperable Train Control.

2.4.1 Description of Message Structure

The structure of the new ITCSM messages differs slightly from that of existing ITCSM messages but still conforms to the EMP standard used for ITCSM, as defined in MSRP S-9354 [2]. The structure used for the new messages was determined with guidance from the ITCSM working group and consisted of:

- The EMP header, called the Interoperable System Management Gateway (ISMG) Header
- The EMP body, called the ISMG Payload consisting of the Service Header and Service Data
- The EMP signature, called the ISMG Signature

Table 1 shows the structure used for the new messages.

Table 1. ITCSM Message Structure for 10303, 10304, 10305, and 10306 Messages

#	Field
EMP Header – Interoperable SMG (ISMG) Header	
1.	Protocol (header) Version
2.	Message Type (ID)
3.	Message Version
4.	Flags
5.	ISMG Data Length
6.	Message Number
7.	Message Time
8.	Variable Header Size
9.	Time To Live
10.	Routing QOS
11.	Source Address
12.	Destination Address
EMP Body – Interoperable SMG (ISMG) Payload	
Service Header	
1.	Protocol (header) Version
2.	Message Type (ID)
3.	Message Version
4.	Flags
5.	Service Data Length
6.	Message Number
7.	Message Time
8.	Variable Header Size
9.	Time to Live
10.	Routing QOS
11.	Source Address
12.	Destination Address
Service Data	
1.	Service Payload Length
2.	Service Payload
3.	Service Signature
EMP Data Integrity – Interoperable SMG (ISMG) Signature	
13.	Interoperable SMG (ISMG) Signature

Currently, other ITCSM messages do not have the "Service Header" section within the EMP body, and all of the fields within the payload are defined within the EMP body and not in a "Service Payload" field. With this two-header structure, some of the functionality of message verification and authentication shifts from the ITCSM System Management Gateway (SMG) to the applications sending and receiving messages. This structure also allows the message service payload to be modified for one or more messages without an update to the SMG software.

2.4.2 ITCSM Data Transfer Request Message 10303

The 10303 Data Transfer Request Message is used to request logs from an asset-owning railroad. This message can be sent by the MAIN-CDX application to an auto railroad, by an auto railroad application to MAIN-CDX, or by an auto railroad directly to another auto railroad. The required data for a manual data request within MAIN-CDX was used as a template to build the service payload fields of the 10303 Data Transfer Request Message. The fields within the "Service Header" and "Service Payload" sections that contain critical information in the 10303 Data Transfer Request Message are described in Table 2 below.

Table 2. 10303 Data Transfer Request Message Key Fields

Field	Description
Service Header	
Message Number	Contains a message number to uniquely identify the request/response pair
Source Address	EMP address of the requesting application
Destination Address	EMP address of the responding application
Service Payload	
Asset Type	Specifies if EMP address or SMID is being provided for asset
Asset ID	Contains EMP address or SMID of the asset containing the data requested
Component ID	Indicates which component of an asset contains the data requested
Time Start	Start time of data requested
Time End	End time of data requested
Requesting Railroad SCAC	SCAC of requesting railroad
Responding Railroad SCAC	SCAC of responding railroad

2.4.3 ITCSM Data Transfer Response Message 10304

The 10304 Data Transfer Response Message is used to respond to a 10303 Data Transfer Request Message. The responding application includes a response code in the 10304 Data Transfer Response Message to indicate to the nature of the response being sent. If the application responds with data, the 10304 Data Transfer Response Message will contain hexadecimal data within the data field representing the ASCII text from the log provided. If the 10303 Data Transfer Request Message is sent to MAIN-CDX, MAIN-CDX is configured to respond with a 10304 Data Transfer Response Message. The fields within the "Service Header" and "Service

Payload" sections that contain critical information in the 10304 Data Transfer Response Message are described in Table 3 below.

Table 3. 10304 Data Transfer Response Message Key Fields

Field	Description
Service Header	
Message Number	Contains the "Message Number" received in the 10303 Data Transfer Request Message that is being responded to
Source Address	EMP address of the responding application
Destination Address	EMP address of the requesting application
Service Payload	
Asset ID	Contains EMP address or SMID of the asset containing the data requested
Component ID	Indicates which component of an asset contains the data requested
Response Code	A value from the domain enumeration "Response Codes" Response Codes: • Complete • Operational Partial • Invalid Asset ID • Invalid Component ID • Invalid Time • Unsupported Message Version • Protocol Error • No Data Available • Denied – No Data Available
Response Text	Comments that pertain to the response message (optional)
Data	The ASCII text of the log data being provided

Each response code, as well as its AG given definition and description, is listed below:

- Complete: This response code is used when responding to a request with data that includes a full record of the start time through the end time. A 10304 Data Transfer Response Message with a response code of "Complete" will close out the request.
- Operational Partial: This response code is used when responding to a request with data that is a partial record of the start time through end time. A 10304 Data Transfer Response Message with a response code of "Operational Partial" will close out the request.
- Invalid Asset ID: This response code is used if the responding railroad does not have an asset with the ID provided. A 10304 Data Transfer Response Message with a response code of "Invalid Asset ID" will close out the request.

- Invalid Component ID: This response code is used if the responding railroad does not have a Component ID associated with the Asset ID. A 10304 Data Transfer Response Message with a response code of "Invalid Component ID" will close out the request.
- Invalid Time: This response code is used if the responding railroad has an issue with the start or end time provided. A 10304 Data Transfer Response Message with a response code of "Invalid Time" will close out the request.
- Unsupported Message Version: This response code is used if the Payload Version is not supported. A 10304 Data Transfer Response Message with a response code of "Unsupported Message Version" will close out the request.
- Protocol Error: This response code is used if there are any issues reading the 10303 Data Transfer Request Message. A 10304 Data Transfer Response Message with a response code of "Protocol Error" will close out the request.
- No Data Available: This response code is used if the data for the request is not currently available. A response code of "No Data Available" will not close the request, but it will allow the requesting application to try again later at the requestor's discretion using the original Service Header Message Number.
- Denied – No Data Available: This response code is used if the request is denied. A 10304 Data Transfer Response Message with response code "Denied – No Data Available" will close out the request.

2.4.4 ITCSM Notification Message 10305

The 10305 Notification Message is used to maintain records of data transfer requests and responses between railroads that utilize auto-to-auto data transfer capability. The 10305 Notification Message is sent by the requesting railroad to MAIN-CDX to report the status of requests, and the responses received in auto-to-auto message transfers. The requesting railroad sends a 10305 Notification Message to MAIN-CDX with every 10304 Data Transfer Response Message received from the responding railroad. MAIN-CDX stores records of every notification message received pertaining to a request. Information contained in the fields of the 10305 Notification Message allows MAIN-CDX to log and track auto-to-auto data transfers. The fields within the "Service Header" and "Service Payload" sections that contain critical information in the 10305 Notification Message are described in Table 4 below.

Table 4. 10305 Notification Message Key Fields

Field	Description
Service Header	
Message Number	Contains the message number used in the auto-to-auto 10303 Data Transfer Request Message
Source Address	EMP address of the application sending the notification
Destination Address	EMP address of the MAIN-CDX application
Service Payload	
Transfer Status	Enumeration indicating the status of the transfer. Transfer Status: • Complete • Operational Partial • Request Initiated • Denied/Invalid • Cancelled
RR SCAC	SCAC of responding railroad
Asset ID	Contains EMP address or SMID of the asset containing the data requested
Component ID	Indicates which component of an asset contains the data requested
Time Start	Start time of data requested
Time End	End time of data requested

Each transfer status, as well as its AG given definition are description, is listed below:

- Complete: This transfer status is used if the 10304 Data Transfer Response Message received from a railroad had a response code of "Complete."
- Operational Partial: This transfer status is used if the 10304 Data Transfer Response Message received from a railroad had a response code of "Operational Partial."
- Request Initiated: This response code is used if the 10304 Data Transfer Response Message received from a railroad had a response code of "No Data Available."
- Denied/Invalid: This response code is used if the 10304 Data Transfer Response Message received any other response code other than "Complete," "Operational Partial," or "No Data Available."
- Cancelled: This response code is used if the requesting railroad is canceling the request. The requesting railroad would have to generate a 10305 Notification Message to MAIN-CDX to update the status of the request on MAIN-CDX to "Cancelled."

2.4.5 ITCSM Notification Response Message 10306

The 10306 Notification Response Message is used to acknowledge a 10305 Notification Message received from an auto railroad. The 10306 Notification Response Message is sent by MAIN-CDX to indicate positive or negative acknowledgement of the notification message sent by the auto requesting railroad. The key fields that contain critical information in the message are described in Table 5 below.

Table 5. 10306 Notification Response Message Key Fields

Field	Description
Service Header	
Message Number	Contains the message number received in the 10305 Notification Message that is being responded to
Source Address	EMP address of the MAIN-CDX application
Destination Address	EMP Address of the application receiving the notification response message
Service Payload	
Notification Response Code	Enumeration indicating positive or negative acknowledgment of the 10305 Notification Message

2.5 Data Transfer Use Cases and Message Flows

The flow of messages between railroads in request/response transfers depends on each railroad's automated transfer capability. Railroads can send and receive requests/responses either manually using the MAIN-CDX application or automatically using ITCSM messages. ITCSM messages are routed from the source application to the destination application through railroad or MAIN-CDX SMGs. The addition of the source and destination addresses within the Service Header fields of the new ITCSM messages allows for routing directly between the applications. Mapping between the 10303 Data Transfer Request Message or the 10304 Data Transfer Response Message and MAIN-CDX is defined in order to handle transfers between automated and manual railroads. The flow of each type of data transfer between both manual and automated railroads is described in the sections below.

2.5.1 MAIN-CDX Manual-to-Manual Message Flow

Manual-to-manual message transfers are executed through the MAIN-CDX application. A manual railroad user fills out the request fields and submits the request on the MAIN-CDX user interface. Once the request is submitted, MAIN-CDX uses information contained within the application to determine if the responding railroad is set up as a manual railroad or an auto railroad. If the railroad is set up as manual, a request notification is sent to the MAIN-CDX users of the asset-owning railroad. Any authorized MAIN-CDX user from the asset-owning railroad can log onto MAIN-CDX to view the request and send a response. The request is shown on the MAIN-CDX dashboard, and the asset-owning railroad can respond to the request by opening the message and filling in the required fields. Once a response is submitted, the status of the request changes, and the requesting railroad receives a notification from the MAIN-CDX application that a response was received. MAIN-CDX will send periodic notification messages to railroads that

have open requests as well as to railroads that have responses containing data that has not yet been downloaded.

2.5.2 MAIN-CDX Manual-to-Auto Message Flow

A diagram of the message flow from the creation of a request by a manual railroad to the response of the request by an auto railroad is shown in Figure 9.

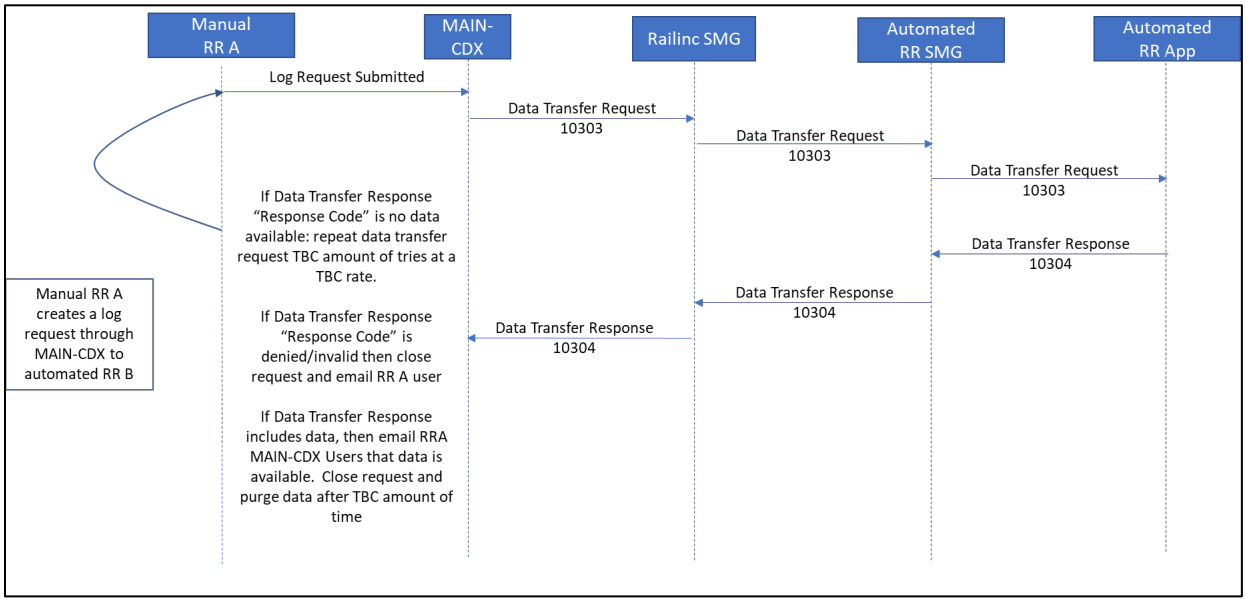


Figure 9. Message Flow Overview for Manual-to-Auto Request/Response

In manual-to-auto message transfers, the manual railroad generates the request manually on the MAIN-CDX user interface. Once the request is submitted, MAIN-CDX uses information contained within the application to determine if the responding railroad is set up as a manual railroad or an auto railroad. If the railroad is set up as an auto railroad, a 10303 Data Transfer Request Message is generated based on the information provided in the MAIN-CDX request. Figure 10 shows boxes around the data from the manually entered request used to generate the 10303 Data Transfer Request Message. Note that for the manually entered request, the railroad has selected four different component IDs. Since the 10303 Data Transfer Request Message is designed to make a request for a single component within an asset, this manual request will generate four different 10303 Data Transfer Request Messages to the responding railroad.

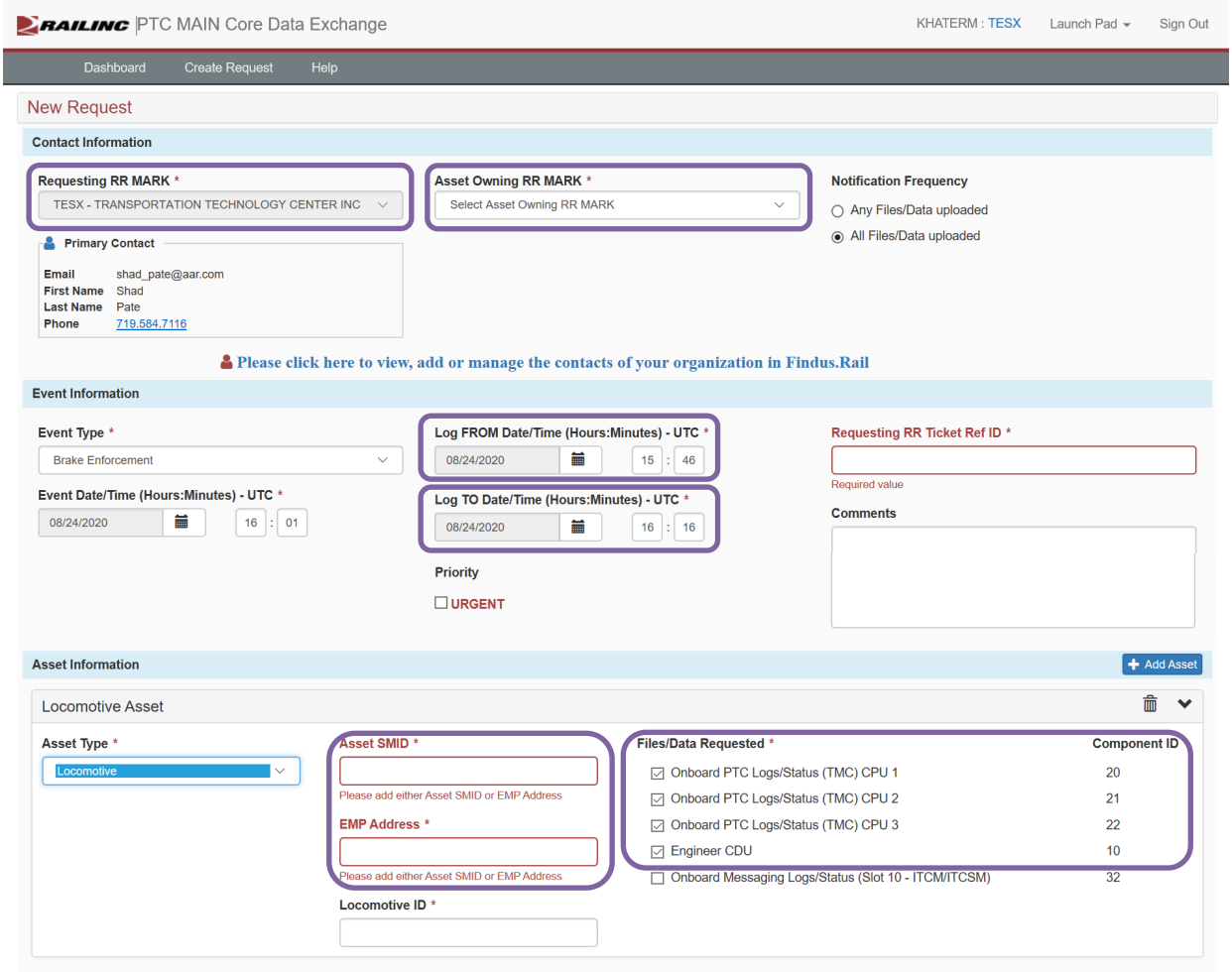


Figure 10. MAIN-CDX Request Fields Used for the 10303 Data Transfer Request Message

After generating a 10303 Data Transfer Request Message, the message is routed to the responding railroad's application. The railroad application receives the request and replies with a 10304 Data Transfer Response Message. The 10304 Data Transfer Response Message is designed so the response will be linked to the 10303 Data Transfer Request Message when populated per the defined requirements. The 10304 Data Transfer Response Message also contains fields where the responding railroad can indicate a response code as well as include response data, if available.

MAIN-CDX uses use the 10304 Data Transfer Response Message to update the request within the MAIN-CDX application based on the information provided within the 10304 Data Transfer Response Message. If the 10304 Data Transfer Response Message contained a response code of "Complete" or "Operational partial," then MAIN-CDX will load the data provided into the request on the application and notify the requesting railroad MAIN-CDX users that data for the request is available. If the response code is "No data available," MAIN-CDX will keep the request pending and re-request later at a to-be-configured (TBC) time. If the response code is anything else, MAIN-CDX updates the status of the request and e-mails the requesting railroad's MAIN-CDX users to review the request and the response provided.

2.5.3 MAIN-CDX Auto-to-Manual Message Flow

A diagram of the message flow from the creation of the request by an auto railroad to the response of a request by a manual railroad is shown in Figure 11.

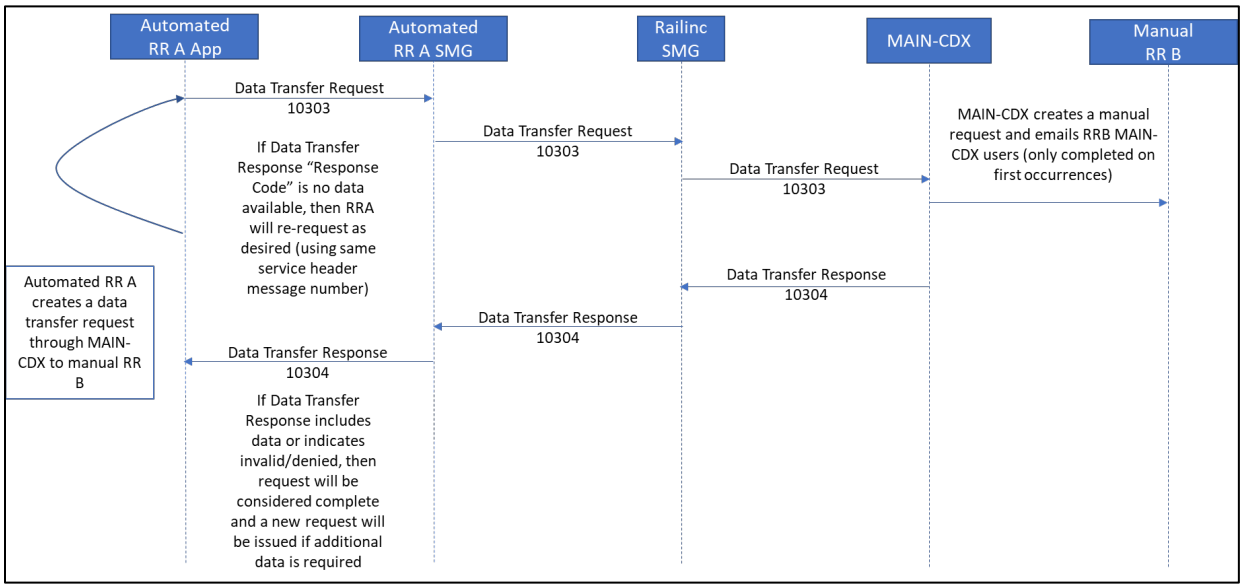


Figure 11. Message Flow Overview for Auto-to-Manual Request/Response

In auto-to-manual message transfers, the auto railroad generates a 10303 Data Transfer Request Message within its application and sends the request to the MAIN-CDX application. Per direction of the AG, all 10303 Data Transfer Request Messages received by MAIN-CDX are turned into a manual request for the responding railroad, regardless of the preference of manual or auto railroad within MAIN-CDX. The intent is that the auto requesting railroad would have sent the request directly to the responding railroad, if it had wanted the request to be an auto request.

Upon receiving the 10303 Data Transfer Request Message, MAIN-CDX uses the contents of the 10303 Data Transfer Request Message to determine if the request already exists in MAIN-CDX. If the request does not exist, MAIN-CDX performs these actions, in the following order:

1. MAIN-CDX parses the contents of the message and populates the data into a manual request directed at the manual railroad.
2. MAIN-CDX creates a 10304 Data Transfer Response Message with a response code of "No data available" and sends it to the requesting railroad's application.
3. MAIN-CDX notifies the responding railroad that a request has been initiated within MAIN-CDX. With the response code set to "No data available," the requesting railroad is responsible for re-requesting at a later time.

If the request already exists, MAIN-CDX creates a 10304 Data Transfer Response Message to the request based on actions taken by the manual railroad since the request was originally created. Various responses could be as follows:

- If the responding railroad has taken no action, MAIN-CDX responds with a 10304 Data Transfer Response Message with a response code of "No data available."

- If the responding railroad has uploaded data and changed the request status, MAIN-CDX creates a 10304 Data Transfer Response Message that includes the appropriate response code along with the text data uploaded for the request.
- If the responding railroad updates the status of the request to invalid or denied, MAIN-CDX creates a 10304 Data Transfer Response Message indicating the status within the response code.

MAIN-CDX sends periodic notifications to the responding railroad's MAIN-CDX users for a request that has not been responded to. MAIN-CDX also notifies the requesting railroad's MAIN-CDX users that a response has been provided if MAIN-CDX has not received another 10303 Data Transfer Request Message within a TBC timeframe.

2.5.4 MAIN-CDX Auto-to-Auto Message Flow

In auto-to-auto message transfers, the auto railroad generates a 10303 Data Transfer Request Message and sends the request directly to the responding railroad. Auto-to-auto request/response message transfers do not need MAIN-CDX to facilitate requests. MAIN-CDX maintains a record of request and response statuses of auto-to-auto message transfers through a 10305 Notification Message sent to MAIN-CDX by the requesting railroad.

The requesting railroad receiving a 10304 Data Transfer Response Message triggers the creation of the 10305 Notification Message to be sent to MAIN-CDX. Data from the 10303 Data Transfer Request Message and the 10304 Data Transfer Response Message determines what the requesting railroad sends in the 10305 Notification Message. MAIN-CDX uses the data from the 10305 Notification Message to log the request, which is then visible on the MAIN-CDX dashboard. Auto railroads can view auto-to-auto requests and responses pertaining to them by selecting the **Show Auto-to-Auto Exchanges** option on the dashboard, seen in Figure 2. MAIN-CDX also responds to the 10305 Notification Message with a 10306 Notification Response Message for acknowledgment purposes. The 10305 Notification Message contains a field for the requesting railroad to indicate the transfer status.

2.6 Data Format

Each railroad has implemented methods to parse and use raw log data for troubleshooting and analysis. For the purpose of sharing data between railroads, the AG decided that raw log data would be used to ensure that a railroad received the same type of data from all railroads. It was also determined that the data would be limited to a single text file when responding with data, placing the responsibility on the responding railroad to concatenate logs files into a single file, if needed.

The AG raised some long-term concerns about using the current logged data for troubleshooting and analysis. The majority of this logged data is vendor-specific, and there is no standardization of what is provided in the logs. These logs have been sufficient for the railroads' troubleshooting and analysis purposes, but changes can be made to the logs as new software is released. Such changes may result in the railroads needing to implement changes to how logs are analyzed. Future efforts to address this concern were discussed and include the creation of industry-standard ITC-PTC logs for desired assets and components or working with the vendors to provide detailed documentation for logs created and maintaining that documentation for each new software release.

2.7 Enhanced Monitoring and Troubleshooting of Foreign Locomotives

The majority of real-time troubleshooting by a railroad's ITC-PTC support desk involves interacting with the crew and locomotive. The host railroad may have different monitoring and troubleshooting capabilities based on whether the locomotive is owned by that railroad or another railroad. Some host railroads have implemented additional monitoring and troubleshooting tools for locomotives owned by that railroad, made possible mainly by accessing the locomotive directly through the railroad's cellular connections. This access is not available to the host railroad for foreign locomotives. For foreign locomotives, the host railroad relies heavily on direct communication with the crew to determine what is taking place on the locomotive.

Based on discussions with the AG, there would be a benefit to developing a tool that would provide a screenshot of the onboard display or temporary remote viewing of the onboard display for use in real-time monitoring and troubleshooting of locomotives. This tool would be limited to only displaying contents of the onboard display and would not allow support desk access to interact with the display.

Future work involving the railroads and vendors will be needed to determine the best method for achieving this. Some options discussed included the creation of new ITC-PTC messages, either Interoperable Train Control Messaging (ITCM) or ITCSM, that would provide a either snapshot of the display or provide display details within the message sufficient to recreate the display. These messages would be triggered by a request from the railroad's back office and would only be sent for a configurable amount of time after the request. Another option included the capability to request temporary streaming of the display from the railroad back office. Currently, railroads can do this for locomotives they own, but it requires that railroad to log in to the onboard system which is not a possibility for foreign locomotives. A process would need to be developed to allow the streaming of information from foreign locomotives.

3. Conclusion

This research project led to and supported the industry with MAIN-CDX, a web application that supports an efficient and standardized method of requesting ITC-PTC asset data from other railroads, responding to requests for data, and tracking request statuses through a dashboard. MAIN-CDX was developed in such a way that it will support railroads using the application to manually enter data requests and responses as well as interact with data requests and responses using the ITCSM messages developed as part of this project. The MAIN-CDX application can also support requests for data and responses to requests between railroads where one railroad's preference is to use the ITCSM messages and the other railroad's preference is to manually use the MAIN-CDX application.

MAIN-CDX has been well-received by the industry and is being used by railroads running ITC-PTC. Railinc plans to continue to support the use of MAIN-CDX and to improve the system based on user feedback.

Currently, the data format used for fulfilling data requests is serving the railroads' needs for troubleshooting and analyzing issues that occur during interoperable operations. As the system matures, there may be a need to work on additional standardization of the data responses and more automation of data analysis. It was also noted that the railroads may gain additional benefit with respect to real-time monitoring and troubleshooting if there was a method or tool available to view the onboard display for all locomotives operating within the railroad's territory.

4. References

Association of American Railroads. (2018). *AAR Manual of Standards and Recommended Practices,* Section K Part V, Standard S-9460, ITCSM Interface Control Document for Interoperable Train Control.

Association of American Railroads. (2018). *AAR Manual of Standards and Recommended Practices,* Section K Part IV, Standard S-9354, Edge Message Protocol.

Appendix A: Proposed ITCSM Data Transfer, Data Response, and Notification Messages Version 0.20

Prepared by TTCI under guidance from the MAIN-CDX advisory group and ITCSM working group, November 2020.

Interim document for 10303, 10304, 10305, and 10306 ITCSM message requirements and specifications.

Example Requirements for Data Transfer Messages

In this section the reader will find:

1. Summary of this approach to Data Transfer messaging
2. Requirements for the structure of the **Data Transfer Request Message** (10303)
3. Requirements for the structure of the **Data Transfer Response Message** (10304)
4. Requirements for the structure of the **Notification Message** (10305)
5. Requirements for the structure of the **Notification Response Message** (10306)
6. MAIN-CDX Payload Structure for 10303, 10304, 10305, and 10306
7. Behavioral requirements for data transfer messages

Summary of This Approach

This approach weighs the idea of creating new ITCSM messages to fulfill the needs of data transfers. This approach aims to create data transfer requests that will meet the needs for application specific uses.

Glossary

Table A1 lists the acronyms used in this document.

Table A1. Acronyms

Acronym	Description
EMP	Edge Message Protocol
HMAC	Hashed Message Authentication Code
ICD	Interface Control Document
Interoperable ISMP message	An ISMP message destined for a foreign gateway or foreign remote agent.
ISMG	Interoperable Systems Management Gateway
ISMG Header	Header field of interoperable ISMP messages sent to a foreign railroad through an ISMG
ISMP	Interoperable Systems Management Protocol
QOS	Quality of Service
ITC	Interoperable Train Control
ITCM	Interoperable Train Control Messaging
ITCSM	ITC Systems Management
ITCSM Gateway	ITC Systems Management Gateway
Interoperable Service	An application providing systems management services for a foreign road.
RR	Railroad
Service Header	An EMP Message header used to identify the sender and recipient of an interoperable ISMP message.
SCAC	Standard Carrier Alpha Code
SMG	Systems Management Gateway

Acronym	Description
SMGA	System Management Gateway Application
SMID	Systems Management Identifier
SMPK	Systems Management Private/Public Key
SMS	System Management System
TTL	Time to Live

Data Transfer Request Message (10303 V1)

Data Transfer Request Message Structure

R1000 The **Data Transfer Request Message** shall have the following structure:

Table A2. Data Transfer Request Message (10303 V1)

#	Field	Size (Bytes)	Type
Interoperable SMG (ISMG) Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	ISMG Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Interoperable SMG (ISMG) Payload			
Service Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	Service Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Service Data			
1.	Service Payload Length	3	Unsigned Int
2.	Service Payload	Variable	
3.	Service Signature	Computed	Binary
Interoperable SMG (ISMG) Signature			
13.	Interoperable SMG (ISMG) Signature	Computed	Binary

Interoperable SMG (ISMG) Header Fields

1. R1005 The **Message Type (ID)** field of the ISMG Header shall contain the value for **Data Transfer Request Message**.
2. R1010 The **Message Version** field of the ISMG Header shall contain the value for the message version of the **Data Transfer Request Message** being used.
3. R1015 The **ISMG Data Length** field of the ISMG Header shall contain a value specifying the size of the ISMG Payload (or the size of the Service Header plus the size of the Service Payload plus the size of the ISMG Signature).
4. R1017 The **Message Number** field of the ISMG Header shall be populated per the requirements specified in the ISMP Design Considerations Document.
   Design Note: The **Data Transfer Request Message** (10303) utilizes a two-header format, the ISMG Header and the Service Header. The Service Header contains message correlation information between the sender and receiver in the **Message Number** field and routing information between the applications in the **Source Address** and **Destination Address** fields. Since routing and correlation data is provided within the Service Header, the need for sessions within the ISMG Header **Message Number** is not needed and as such, a session ID of 0 shall be used for the 10303 messages.
5. R1020 The **Source Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component sending the message.
6. R1030 The **Destination Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component receiving the message.
7. R1040 The other fields of the ISMG Header shall be populated per the EMP specification for a message with no EMP Data Integrity support.

Service Header Fields

1. R1045 The **Protocol (Header) Version** field of the Service Header shall be set to 1 for the *Data Transfer Request Message*.
2. R1050 The **Message Type (ID)** field of the *Service Header* shall be the same value as the ***Message Version (ID)*** field of the *ISMG Header*.
3. R1060 The **Message Version** field of the *Service Header* shall be the same value as the ***Message Version*** field of the *ISMG Header*.
4. R1065 The ***Service Data Length*** field of the *Service Header* shall contain a value specifying the size of the Service Data.
5. R1067 The ***Message Number*** field of the Service Header shall contain a 32-bit value to uniquely identify the request/response pair.
6. R1070 The **Source Address** field of the Service Header shall contain a value specifying the EMP Address of the Requesting Application (scac.b:mcdx or scac.b:<RR specific>).
   Design Note: The Source Address does not update during hops between SMGs and is used to identify the sender of the message.
   Design Note: The EMP address for the Main CDX service shall be of the format scac.b:mcdx and the EMP address for the RR service shall be of the format scac.b:<RR specific>.
7. R1080 The **Destination Address** field of the Service Header shall contain a value specifying the EMP address of the Responding Application (scac.b:<RR specific> or scac.b:mcdx).

Design Note: The Destination Address does not update during hops between SMGs.

8. R1090 The other fields of the *Service Header* shall be populated per the EMP specification.

Service Payload Fields

1. R1120 The **Service Payload Length** field shall contain a value specifying the length of the **Service Payload** field.
2. R1130 The **Service Payload** field shall contain application specific fields as documented for the application using the **Data Transfer Request Message**.
   Design Note: The first field within the **Service Payload** must be an **Application Payload Version** specifying the version of the **Data Transfer Notification Message** payload.
   Design Note: The **Service Payload** for the Data Transfer Request Message for MAIN-CDX's use is defined in Section 6.1.

Signatures

1. R1200 The ***Service Signature*** field shall contain an SMPK Signature calculated over the Service Header and Service Data.
   Design Note: The Service Signature does not change over SMG hops and will be used to validate the sender of the message once SMGA-2 is implemented.
2. R1210 The ***Interoperable SMG (ISMG) Signature*** field shall contain an SMPK Signature calculated over the ISMG Header and ISMG Payload.
   Design Note: The ISMG Signature will be verified and updated by the Gateway at each hop per the SMGA-1 behavior.

Message Routing Behavior

1. R1220 The Domestic Gateway shall use the public key associated with the **Source Address** field in the Interoperable SMG (ISMG) Header to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.
2. R1230 The Domestic Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Gateway. The "Source Address" field of the updated ISMG Header shall be populated with the Domestic Gateway's EMP Address. The **Destination Address** of the updated ISMG Header shall be determined by using the SCAC portion of the **Destination Address** field in the Service Header.
3. R1231 The Domestic Gateway shall sign the message in the **Interoperable SMG (ISMG) Signature** (SMPK) field using the private key of the Domestic Gateway.
4. R1240 The Foreign Gateway shall use the public key associated with the **Source Address** field in the Interoperable SMG (ISMG) Header to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field
5. R1250 The Foreign Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Back Office Application. The **Source Address** field of the updated ISMG Header shall be populated with the Foreign Gateway's EMP Address. The **Destination Address** of the updated ISMG Header shall be populated with the **Destination Address** field in the Service Header.
   Design Note: The **Destination Address** field in the Service Header will have an EMP address for the destined application, which will be used to determine where the foreign gateway is going to route the message. The intent is that the underlying transport mechanisms provide dedicated queues only associated with the destination address and

not a general delivery requiring the service to pull its messages from a mix of other messages.

6. R1251 The Foreign Gateway shall sign the message in the **Interoperable SMG (ISMG) Signature** (SMPK) field using the private key of the Foreign Gateway.
7. R1260 The Application shall use the public key associated with the Foreign Gateway to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.

Data Transfer Response Message (10304 V1)

Data Transfer Response Message Structure

R1500 The **Data Transfer Response** message shall have the following structure:

Table A3. Data Transfer Response Message (10304 V1)

#	Field	Size (Bytes)	Type
Interoperable SMG (ISMG) Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	ISMG Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Interoperable SMG (ISMG) Payload			
Service Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	Service Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Service Data			
1.	Service Payload Length	3	Unsigned Int
2.	Service Payload	Variable	
3.	Service Signature	Computed	Binary
Interoperable SMG (ISMG) Signature			
13.	Interoperable SMG (ISMG) Signature	Computed	Binary

Interoperable SMG (ISMG) Header Fields

1. R1505 The **Message Type (ID)** field of the ISMG Header shall contain the value for **Data Transfer Response Message**.
2. R1510 The **Message Version** field of the ISMG Header shall contain the value for the message version of the **Data Transfer Response Message** being used.
3. R1515 The **ISMG Data Length** field of the ISMG Header shall contain a value specifying the size of the ISMG Payload (or the size of the Service Header plus the size of the Service Payload plus the size of the ISMG Signature).
4. R1517 The **Message Number** field of the ISMG Header shall be populated per the requirements specified in the ISMP Design Considerations Document.
   Design Note: The Data Transfer Response Message (10304) utilizes a two-header format, the ISMG Header and the Service Header. The Service Header contains message correlation information between the sender and receiver in the **Message Number** field and routing information between the applications in the **Source Address** and **Destination Address** fields. Since routing and correlation data is provided within the Service Header, the need for sessions within the ISMG Header **Message Number** is not needed and as such, a session ID of 0 shall be used for the 10304 messages.
5. R1520 The **Source Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component sending the message.
6. R1530 The **Destination Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component receiving the message.
7. R1540 The other fields of the ISMG Header shall be populated per the EMP specification for a message with no EMP Data Integrity support.

Service Header Fields

1. R1545 The **Protocol (Header) Version** field of the Service Header shall be set to 1 for the Data Transfer Response Message.
2. R1550 The **Message Type (ID)** field of the Service Header shall be the same value as the **Message Version (ID)** field of the ISMG Header.
3. R1560 The **Message Version** field of the Service Header shall be the same value as the **Message Version** field of the ISMG Header.
4. R1565 The **Service Data Length** field of the Service Header shall contain a value specifying the size of the Service Data.
5. R1567 The **Message Number** field of the Service Header shall contain the **Message Number** received in the **Date Transfer Request Message** that is being responded to.
6. R1570 The **Source Address** field of the Service Header shall contain a value specifying the EMP Address of the Responding Application (scac.b:mcdx or scac.b:<RR specific>).
   Design Note: The Source Address does not update during hops between SMGs and is used to identify the sender of the message.
7. R1580 The **Destination Address** field of the Service Header shall contain a value specifying the EMP address of the Requesting Application (scac.b:<RR Specific> or scac.b:mcdx).
   Design Note: The Destination Address does not update during hops between SMGs.
8. R1590 The other fields of the Service Header shall be populated per the EMP specification.

Service Payload Fields

1. R1620 The **Service Payload Length** field shall contain a value specifying the length of the **Service Payload** field.
2. R1630 The **Service Payload** field shall contain application specific fields as documented for the application using the **Data Transfer Response Message**.
   Design Note: The first field within the **Service Payload** must be an **Application Payload Version** specifying the version of the **Data Transfer Notification Message** payload.
   Design Note: The **Service Payload** for the Data Transfer Response Message for MAIN-CDX's use is defined in Section 6.2.

Signatures

1. R1700 The ***Service Signature*** field shall contain an SMPK Signature calculated over the Service Header and Service Data.
   Design Note: The Service Signature does not change over SMG hops and will be used to validate the sender of the message once SMGA-2 is implemented.
2. R1710 The ***Interoperable SMG (ISMG) Signature*** field shall contain an SMPK Signature calculated over the ISMG Header and ISMG Payload.
   Design Note: The ISMG Signature will be verified and updated by the Gateway at each hop per the SMGA-1 behavior.

Message Routing Behavior

1. R1720 The Domestic Gateway shall use the public key associated with the Source Address field in the Interoperable SMG (ISMG) Header to verify the Interoperable SMG (ISMG) Signature (SMPK) field.
2. R1730 The Domestic Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Gateway. The Source Address field of the updated ISMG Header shall be populated with the Domestic Gateway's EMP Address. The Destination Address of the updated ISMG Header shall be determined by using the SCAC portion of the Destination Address field in the Service Header.
3. R1731 The Domestic Gateway shall sign the message in the Interoperable SMG (ISMG) Signature (SMPK) field using the private key of the Domestic Gateway.
4. R1740 The Foreign Gateway shall use the public key associated with the Source Address field in the Interoperable SMG (ISMG) Header to verify the Interoperable SMG (ISMG) Signature (SMPK) field.
5. R1750 The Foreign Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Back Office Application. The **Source Address** field of the updated ISMG Header shall be populated with the Foreign Gateway's EMP Address. The **Destination Address** of the updated ISMG Header shall be populated with the **Destination Address** field in the Service Header.
   design note: the **destination address** field in the service header will have an emp address for the destined application, which will be used to determine where the foreign gateway is going to route the message. The intent is that the underlying transport mechanisms provide dedicated queues only associated with the destination address and not a general delivery requiring the service to pull its messages from a mix of other messages.
6. R1751 The Foreign Gateway shall sign the message in the **Interoperable SMG (ISMG) Signature** (SMPK) field using the private key of the Foreign Gateway.

7. R1760 The Application shall use the public key associated with the Foreign Gateway to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.

Notification Message (10305 V1)

Notification Message Structure

R2000 The **Notification** message shall have the following structure:

Table A4. Notification Message (10305 V1)

#	Field	Size (Bytes)	Type
Interoperable SMG (ISMG) Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	ISMG Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Interoperable SMG (ISMG) Payload			
Service Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	Service Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Service Data			
1.	Service Payload Length	3	Unsigned Int
2.	Service Payload	Variable	
3.	Service Signature	Computed	Binary
Interoperable SMG (ISMG) Signature			
13.	Interoperable SMG (ISMG) Signature	Computed	Binary

Interoperable SMG (ISMG) Header Fields

1. R2005 The **Message Type (ID)** field of the ISMG Header shall contain the value for **Notification Message**.
2. R2010 The **Message Version** field of the ISMG Header shall contain the value for the message version of the **Notification Message** being used.
3. R2015 The **ISMG Data Length** field of the ISMG Header shall contain a value specifying the size of the ISMG Payload (or the size of the Service Header plus the size of the Service Payload plus the size of the ISMG Signature).
4. R2017 The **Message Number** field of the ISMG Header shall be populated per the requirements specified in the ISMP Design Considerations Document.
   Design Note: The **Notification Message** (10305) utilizes a two-header format, the ISMG Header and the Service Header. The Service Header contains message correlation information between the sender and receiver in the **Message Number** field and routing information between the applications in the **Source Address** and **Destination Address** fields. Since routing and correlation data is provided within the Service Header, the need for sessions within the ISMG Header **Message Number** is not needed and as such, a session ID of 0 shall be used for the 10305 messages.
5. R2020 The **Source Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component sending the message.
6. R2030 The **Destination Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component receiving the message.
7. R2040 The other fields of the ISMG Header shall be populated per the EMP specification for a message with no EMP Data Integrity support.

Service Header Fields

1. R2045 The **Protocol (Header) Version** field of the Service Header shall be set to 1 for the *Notification Message*.
2. R2050 The **Message Type (ID)** field of the *Service Header* shall be the same value as the ***Message Version (ID)*** field of the *ISMG Header*.
3. R2060 The **Message Version** field of the *Service Header* shall be the same value as the ***Message Version*** field of the *ISMG Header*.
4. R2065 The ***Service Data Length*** field of the *Service Header* shall contain a value specifying the size of the Service Data.
5. R2067 The ***Message Number*** field of the Service Header shall contain a 32-bit value to uniquely identify the notification.
   Design Note: Update notifications will use the ***Message Number*** sent in the first notification.
6. R2070 The **Source Address** field of the Service Header shall contain a value specifying the EMP Address of the Application sending the notification scac.b:<RR specific>.
   Design Note: The Source Address does not update during hops between SMGs and is used to identify the sender of the message.
7. R2080 The **Destination Address** field of the Service Header shall contain a value specifying the EMP address of the Application receiving the notification (scac.b:mcdx).
   Design Note: The Destination Address does not update during hops between SMGs.
8. R2090 The other fields of the *Service Header* shall be populated per the EMP specification.

Service Payload Fields

1. R2120 The **Service Payload Length** field shall contain a value specifying the length of the **Service Payload** field.
2. R2130 The **Service Payload** field shall contain application specific fields as documented for the application using the **Notification Message**.
   Design Note: The first field within the **Service Payload** must be an **Application Payload Version** specifying the version of the **Notification Message** payload.
   Design Note: The **Service Payload** for the Notification Message for MAIN-CDX's use is defined in Section 6.3.

Signatures

1. R2200 The ***Service Signature*** field shall contain an SMPK Signature calculated over the Service Header and Service Data.
   Design Note: The Service Signature does not change over SMG hops and will be used to validate the sender of the message once SMGA-2 is implemented.
2. R2210 The ***Interoperable SMG (ISMG) Signature*** field shall contain an SMPK Signature calculated over the ISMG Header and ISMG Payload.
   Design Note: The ISMG Signature will be verified and updated by the Gateway at each hop per the SMGA-1 behavior.

Message Routing Behavior

1. R2220 The Domestic Gateway shall use the public key associated with the Source Address field in the Interoperable SMG (ISMG) Header to verify the Interoperable SMG (ISMG) Signature (SMPK) field.
2. R2230 The Domestic Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Gateway. The Source Address field of the updated ISMG Header shall be populated with the Domestic Gateway's EMP Address. The Destination Address of the updated ISMG Header shall be determined by using the SCAC portion of the Destination Address field in the Service Header.
3. R2231 The Domestic Gateway shall sign the message in the Interoperable SMG (ISMG) Signature (SMPK) field using the private key of the Domestic Gateway.
4. R2240 The Foreign Gateway shall use the public key associated with the Source Address field in the Interoperable SMG (ISMG) Header to verify the Interoperable SMG (ISMG) Signature (SMPK) field.
5. R2250 The Foreign Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Back Office Application. The Source Address field of the updated ISMG Header shall be populated with the Foreign Gateway's EMP Address. The Destination Address of the updated ISMG Header shall be populated with the Destination Address field in the Service Header.
   Design Note: The Destination Address field in the Service Header will have an EMP address for the destined application, which will be used to determine where the foreign gateway is going to route the message. The intent is that the underlying transport mechanisms provide dedicated queues only associated with the destination address and not a general delivery requiring the service to pull its messages from a mix of other messages.

6. R2251 The Foreign Gateway shall sign the message in the Interoperable SMG (ISMG) Signature (SMPK) field using the private key of the Foreign Gateway.
7. R2260 The Application shall use the public key associated with the Foreign Gateway to verify the Interoperable SMG (ISMG) Signature (SMPK) field.

Notification Response Message (10306 V1)

Notification Response Message Structure

R2500 The **Notification Response** message shall have the following structure:

Table A5. Notification Message (10306 V1)

#	Field	Size (Bytes)	Type
Interoperable SMG (ISMG) Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	ISMG Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Interoperable SMG (ISMG) Payload			
Service Header			
1.	Protocol (header) Version	1	Unsigned Int
2.	Message Type (ID)	2	Unsigned Int
3.	Message Version	1	Unsigned Int
4.	Flags	1	Binary
5.	Service Data Length	3	Unsigned Int
6.	Message Number	4	Unsigned Int
7.	Message Time	4	Unsigned Int
8.	Variable Header Size	1	Unsigned Int
9.	Time to Live	2	Unsigned Int
10.	Routing QOS	2	Binary
11.	Source Address	1-64	US ASCII
12.	Destination Address	1-64	US ASCII
Service Data			
1.	Service Payload Length	3	Unsigned Int
2.	Service Payload	Variable	
3.	Service Signature	Computed	Binary
Interoperable SMG (ISMG) Signature			
13.	Interoperable SMG (ISMG) Signature	Computed	Binary

Interoperable SMG (ISMG) Header Fields

1. R2505 The **Message Type (ID)** field of the ISMG Header shall contain the value for **Notification Response Message**.
2. R2510 The **Message Version** field of the ISMG Header shall contain the value for the message version of the **Notification Response Message** being used.
3. R2515 The **ISMG Payload Length** field of the ISMG Header shall contain a value specifying the size of the ISMG Payload (or the size of the Service Header plus the size of the Service Payload plus the size of the ISMG Signature).
4. R2517 The **Message Number** field of the ISMG Header shall be populated per the requirements specified in the ISMP Design Considerations Document.
   Design Note: The **Notification Response Message** (10306) utilizes a two-header format, the ISMG Header and the Service Header. The Service Header contains message correlation information between the sender and receiver in the **Message Number** field and routing information between the applications in the **Source Address** and **Destination Address** fields. Since routing and correlation data is provided within the Service Header, the need for sessions within the ISMG Header **Message Number** is not needed and as such, a session ID of 0 shall be used for the 10306 messages.
5. R2520 The **Source Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component sending the message.
6. R2530 The **Destination Address** field of the ISMG Header shall contain a value specifying the EMP Address of the component receiving the message.
7. R2540 The other fields of the ISMG Header shall be populated per the EMP specification for a message with no EMP Data Integrity support.

Service Header Fields

1. R2545 The **Protocol (Header) Version** field of the Service Header shall be set to 1 for the ***Notification Response Message***.
2. R2550 The **Message Type (ID)** field of the *Service Header* shall be the same value as the ***Message Version (ID)*** field of the *ISMG Header*.
3. R2560 The **Message Version** field of the *Service Header* shall be the same value as the ***Message Version*** field of the *ISMG Header*.
4. R2565 The ***Service Data Length*** field of the *Service Header* shall contain a value specifying the size of the Service Data.
5. R2567 The ***Message Number*** field of the Service Header shall contain the value specified in the ***Message Number*** field from the Notification Message.
   Design Note: Update notifications will use the "Message Number" sent in the first notification.
6. R2570 The **Source Address** field of the Service Header shall contain a value specifying the EMP Address of the application sending the Notification Response message (scac.b:mcdx).
   Design Note: The Source Address does not update during hops between SMGs and is used to identify the sender of the message.
7. R2580 The **Destination Address** field of the Service Header shall contain a value specifying the EMP address of the Application that sent the Notification Request (scac.b:<RR specific>).
   Design Note: The Destination Address does not update during hops between SMGs.

8. R2590 The other fields of the *Service Header* shall be populated per the EMP specification.

Service Payload Fields

1. R2620 The **Service Payload Length** field shall contain a value specifying the length of the **Service Payload** field.
2. R2630 The **Service Payload** field shall contain application specific fields as documented for the application using the **Notification Response Message**.
   Design Note: The first field within the **Service Payload** must be an **Application Payload Version** specifying the version of the Notification Response Message payload.
   Design Note: The **Service Payload** for the Notification Response Message for MAIN-CDX's use is defined in Section 6.4.

Signatures

1. R2700 The ***Service Signature*** field shall contain an SMPK Signature calculated over the Service Header and Service Data.
   Design Note: The Service Signature does not change over SMG hops and will be used to validate the sender of the message once SMGA-2 is implemented.
2. R2710 The ***Interoperable SMG (ISMG) Signature*** field shall contain an SMPK Signature calculated over the ISMG Header and ISMG Payload.
   Design Note: The ISMG Signature will be verified and updated by the Gateway at each hop per the SMGA-1 behavior.

Message Routing Behavior

3. R2720 The Domestic Gateway shall use the public key associated with the **Source Address** field in the Interoperable SMG (ISMG) Header to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.
4. R2730 The Domestic Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Gateway. The **Source Address** field of the updated ISMG Header shall be populated with the Domestic Gateway's EMP Address. The **Destination Address** of the updated ISMG Header shall be determined by using the SCAC portion of the **Destination Address** field in the Service Header.
5. R2731 The Domestic Gateway shall sign the message in the **Interoperable SMG (ISMG) Signature** (SMPK) field using the private key of the Domestic Gateway.
6. R2740 The Foreign Gateway shall use the public key associated with the **Source Address**s field in the Interoperable SMG (ISMG) Header to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.
7. R2750 The Foreign Gateway will modify the Interoperable SMG (ISMG) Header (EMP Header) and update it for routing to the Foreign Back Office Application. The **Source Address** field of the updated ISMG Header shall be populated with the Foreign Gateway's EMP Address. The **Destination Address** of the updated ISMG Header shall be populated with the **Destination Address** field in the Service Header.
   Design Note: The **Destination Address** field in the Service Header will have an EMP address for the destined application, which will be used to determine where the foreign gateway is going to route the message. The intent is that the underlying transport mechanisms provide dedicated queues only associated with the destination address and

not a general delivery requiring the service to pull its messages from a mix of other messages.

8. R2751 The Foreign Gateway shall sign the message in the **Interoperable SMG (ISMG) Signature** (SMPK) field using the private key of the Foreign Gateway.
9. R2760 The Application shall use the public key associated with the Foreign Gateway to verify the **Interoperable SMG (ISMG) Signature** (SMPK) field.

Payload Structures for MAIN-CDX use of 10303, 10304, 10305, and 10306

Data Transfer Request Payload Structure (V1)

Table A6. Data Transfer Request Payload Fields

	Field Names	Size (Byte)	Type
1.	Application Payload Version	1	Unsigned Int
2.	Asset ID Type	1	Enum
3.	Asset ID Length	1	Unsigned Int
4.	Asset ID	Variable	US ASCII
5.	Component ID	1	Unsigned Int
6.	Time Start	14	US ASCII
7.	Time End	14	US ASCII
8.	Requesting RR SCAC Length	1	Unsigned Int
9.	Requesting RR SCAC	4 max	US ASCII
10.	Responding RR SCAC Length	1	Unsigned Int
11.	Responding RR SCAC	4 max	US ASCII

1. R3000 The ***Application Payload Version*** field of the *Data Transfer Request Payload* shall contain the value for the version of the *Data Transfer Request Payload* being used by the application.
   Design Note: The ***Application Payload Version*** will be used to determine the fields required within the payload, based on application specific documentation.
2. R3005 The ***Asset ID Type*** field shall contain a value from the domain enumeration ***Asset ID Types***.
   Asset ID Types
   - SMID – 0x00
   - EMP address – 0x01
3. R3010 The ***Asset ID Length*** field shall contain a value specifying the length of the ***Application ID*** field.
4. R3020 The ***Asset ID*** field shall contain either the SMID or EMP address of the asset containing the data being requested.
5. R3030 The ***Component ID*** field shall be zero for Assets without components.
6. R3031 The ***Component ID*** field shall indicate which component of an Asset is associated with the data request for Assets comprised of multiple components.
7. R3032 The ***Component ID*** field shall contain a value as specified in the Asset Specific Data Dictionaries.
8. R3040 The ***Time Start*** field shall contain a value specifying the start time of the data being requested.
9. R3050 The ***Time End*** field shall contain a value specifying the end time of the data being requested.
10. Design Note: The ***Time Start*** and ***Time End*** fields shall be in ISO8601 format with no separators to the nearest minute in UTC time (yyymmddThhmmZ).

11. R3060 The ***Requesting RR SCAC Length*** field shall contain a value specifying the length of the ***Requesting RR SCAC*** field. If the ***Requesting RR SCAC*** is not provided then the ***Requesting RR SCAC Length*** field shall be set to 0.
12. R3070 The ***Requesting RR SCAC*** field shall contain a value specifying the SCAC of the requesting railroad.
13. R3080 The ***Responding RR SCAC Length*** field shall contain a value specifying the length of the ***Responding RR SCAC*** field. If the ***Responding RR SCAC*** is not provided then the ***Responding RR SCAC Length*** field shall be set to 0.
14. R3090 The ***Responding RR SCAC*** field shall contain a value specifying the SCAC of the responding railroad.

Data Transfer Response Payload Structure (V1)

Table A7. Data Transfer Response Payload Fields

	Field Names	**Size (Byte)**	**Type**
1.	Application Payload Version	1	Unsigned Int
2.	Asset ID Length	1	Unsigned Int
3.	Asset ID	Variable	US ASCII
4.	Component ID	1	Unsigned Int
5.	Response Code	1	Enum
6.	Response Text Length	1	Unsigned Int
7.	Response Text	Variable	US ASCII
8.	Data Length	3	Unsigned Int
9.	Data	Variable	Binary

1. R3500 The ***Application Payload Version*** field of the *Data Transfer Response Payload* shall contain the value for the version of the *Data Transfer Response Payload* being used by the application.
   Design Note: The ***Application Payload Version*** will be used to determine the fields required within the payload, based on application specific documentation.
2. R3510 The ***Asset ID Length*** field shall contain a value specifying the length of the ***Application ID*** field.
3. R3520 The ***Asset ID*** field shall contain either the SMID or EMP address of the asset containing data being requested.
4. R3530 The ***Component ID*** field shall contain a value specifying the component of interest from the asset identified in the ***Asset ID*** field.
   Design Note: The ***Component ID*** will be zero for assets that do not have multiple components.
5. R3540 The ***Response Code*** field shall contain a value from the domain enumeration ***Response Codes***.

Response Codes

- Complete – 0x00
- Operational partial – 0x03
- Invalid Asset ID – 0x01
- Invalid Component ID/Component Not Supported on System – 0xDA
- Invalid time – 0x30
- Unsupported message version – 0x20
- Protocol error/Service Payload Error – 0x19
- No data available – 0x31
- Denied – No data available – 0x32

Notice: Response codes have been added for developmental and testing purposes. These codes will change based on final ITCSM documentation.

6. R3550 The ***Response Text Length*** field shall contain a value specifying the length of the ***Response Text*** field.
7. R3560 The ***Response Text*** field is optional and shall contain comments in US ASCII that pertain to the response. If there is no comments in the ***Response Text*** field, then the ***Response Text Length*** field shall bet set to 0.
8. R3570 The ***Data Length*** field shall contain a value specifying the length of the ***Data*** field.
9. R3580 The ***Data*** field shall contain the data being transferred.
   Design Note: The ***Data*** will need to be limited so that the entire *Data Transfer Response Message does not exceed* 16 MB.

Notification Payload Structure (V1)

Table A8. Notification Message Payload Fields

	Field Names	**Size (Byte)**	**Type**
1.	Application Payload Version	1	Unsigned Int
2.	Transfer Status	1	Enum
3.	RR SCAC Length	1	Unsigned Int
4.	RR SCAC	4 max	US ASCII
5.	Asset ID Length	1	Unsigned Int
6.	Asset ID	Variable	US ASCII
7.	Component ID	1	Unsigned Int
8.	Time Start	14	US ASCII
9.	Time End	14	US ASCII

1. R4000 The ***Application Payload Version*** field of the *Notification Payload* shall contain the value for the version of the *Notification Payload* being used by the application.
   Design Note: The ***Application Payload Version*** will be used to determine the fields required within the payload, based on application specific documentation.

2. R4010 The ***Transfer Status*** field shall contain an enumeration indicating the status of the transfer.
   Transfer Statuses
   - Complete – 0x00
   - Operational partial – 0x03
   - Request initiated – 0x01
   - Denied/Invalid – 0x02
   - Cancelled – 0x04

   Notice: Transfer status codes values have been added. Will need TAG feedback for if these should be different or not. Currently have these codes separate from "Response Codes" in ITCSM documentation
3. R4020 The ***RR SCAC Length*** field shall contain a value specifying the length of the ***RR SCAC*** field.
4. R4030 The ***RR SCAC*** field shall contain a value specifying the SCAC of the responding railroad.
5. R4040 The ***Asset ID Length*** field shall contain a value specifying the length of the ***Application ID*** field.
6. R4050 The ***Asset ID*** field shall contain either the SMID or EMP address of the asset containing data being requested.
7. R4060 The ***Component ID*** field shall be zero for Assets without components.
8. R4061 The ***Component ID*** field shall indicate which component of an Asset is associated with the data request for Assets comprised of multiple components.
9. R4062 The ***Component ID*** field shall contain a value as specified in the Asset Specific Data Dictionaries.
10. R4070 The ***Time Start*** field shall contain a value specifying the start time of the data being requested.
11. R4080 The ***Time End*** field shall contain a value specifying the end time of the data being requested.
    Design Note: The ***Time Start*** and ***Time End*** fields shall be in ISO8601 format with no separators to the nearest minute in UTC time (yyymmddThhmmZ).

Notification Response Payload Structure (V1)

Table A9. Notification Response Payload Fields

	Field Names	Size (Byte)	Type
1.	Application Payload Version	1	Unsigned Int
2.	Notification Response Code	1	Enum

1. R4000 The ***Application Payload Version*** field of the *Notification Response Payload* shall contain the value for the version of the *Notification Response Payload* being used by the application.
2. Design Note: The ***Application Payload Version*** will be used to determine the fields required within the payload, based on application specific documentation.

Notice: Notification response codes values have been added. Will need TAG feedback for if these should be different or not. Currently have these codes separate from "Response Codes" in ITCSM documentation.

3. R4010 The ***Notification Response Code*** field shall contain an enumeration indicating the acknowledgment or negative acknowledgment of the Notification Message.
   Notification Response Codes
   - Acknowledge – 0x00
   - Negative Acknowledge – 0x01

Behavioral Requirements

For all security related issues, the gateway or application shall log the error and discard the message (e.g., invalid signature).

For all other issues within the gateway, the gateway shall log the error and discard the message (e.g., malformed EMP header, unable to send the message next destination, etc.).

Behavioral Requirements for Data Transfer Requests (10303)

Client APP to SMG

1. A Data Transfer Request (10303) shall be generated by Client APP and sent to Domestic SMG.
2. Domestic SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the error and no response will be sent back to Client APP.
   - If signature is validated, then Domestic SMG continues to process message.
3. The Domestic SMG shall validate the ISMG header as well as the SCAC from the ***"Destination Address"*** field of the Service Header.
   - If validation fails, then the SMG shall log the error and no response will be sent back to the Client APP.
   - If the session ID within the ***Message Number*** field of the ISMG Header is something other than 0, then the SMG shall log the error and no response will be sent back to the client APP.
   - If ISMG header and SCAC are validated, then SMG continues to process message.

SMG to SMG

1. Domestic SMG shall send 10303 message to Foreign SMG.
   - If Foreign SMG is not configured in Domestic SMG, then the SMG will log the error and no response shall be sent back to Client APP.
2. Foreign SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the error and no response will be sent back to Domestic SMG.
   - If signature is validated, then Foreign SMG continues to process message.
3. Foreign SMG shall send message to EMP address in the ***Destination Address*** field in the service header.
   - If the ***Destination Address*** is an invalid EMP address, then the Foreign SMG will log the error and no response will be generated.

SMG to Client APP

1. A Data Transfer Request (10303) shall be sent to the ***Destination Address*** (Client APP) field in the Service header once the message has been received from a foreign SMG and validated.
2. The Client APP shall validate the ISMG signature.
   - If signature validation fails, the Client APP shall log the failure and no response shall be sent back to SMG.
   - If signature is validated, then the Client APP continues to process message.

3. The Client APP shall validate that the requesting RR is a valid system user.
    - If requesting RR is not a valid system user, then Client APP shall log the error and no response shall be sent back to SMG.
    - If requesting RR is a valid system user, then Client APP shall continue to process message.

Client APP Validation of Data Transfer Request

1. The Client APP shall validate the Service Header fields.
    - If any of the Service header fields are malformed, the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Protocol error"* in the service payload.
    - If the ***Message Version*** of the Service Header is invalid, then the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Unsupported message version"* in the service payload.
    - If the value in the ***Time to Live*** field of the Service Header is less than the difference between current time and the time in the ***Message Time*** of the service header, then log the error and no response message shall be sent back.
    - If Service Header fields are validated, then Client APP shall continue to process message.
2. The Client APP shall validate the Service Payload fields.
    - If any of the Service Payload fields are malformed, the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Service Payload error"* in the service payload.
    - If the ***Application Version*** of the Service Payload is invalid, then the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Unsupported message version"* in the service payload.
    - If the ***Asset ID*** of the Service Payload is invalid, then the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Invalid Asset ID"* in the service payload.
    - If the ***Component ID*** of the Service Payload is invalid, then the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Invalid Component ID"* in the service payload.
    - If the ***Date Request Time Start*** or the ***Date Request Time End*** fields of the Service Payload are invalid, then then the Client APP shall log the error and respond with a Data Transfer Response (10304) with a ***Response Code*** of *"Invalid time"* in the service payload.
    - If the Service payload fields are validated, then the Client APP should process the message and respond based on the Application-to-Application behavior requirements.

Behavioral Requirements for Data Transfer Response (10304)

Client APP to SMG

1. A Data Transfer Response (10304) shall be generated by Client APP and sent to Domestic SMG.
2. Domestic SMG shall validate the ISMG signature.

- If signature validation fails, the SMG shall log the failure and no response will be sent back to Client APP.
- If signature is validated, then Domestic SMG continues to process message.

3. The Domestic SMG shall validate the ISMG header as well as the SCAC from the ***Destination Address*** field of the Service Header.
   - If validation fails, then the SMG shall log the failure and no response will be sent back to the Client APP.
   - If the session ID within the ***Message Number*** field of the ISMG Header is something other than 0, then the SMG shall log the error and no response will be sent back to the client APP.
   - If ISMG header and SCAC are validated, then SMG continues to process message.

SMG to SMG

1. Domestic SMG shall send 10304 message to Foreign SMG.
   - If Foreign SMG is not configured in Domestic SMG, then the SMG will log the error and no response shall be sent back to Client APP.
2. Foreign SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the error and no response will be sent back to Domestic SMG.
   - If signature is validated, then Foreign SMG continues to process message.
3. Foreign SMG shall send message to EMP address in the ***Destination Address*** field in the service header.
   - If the ***Destination Address*** is an invalid EMP address, then the Foreign SMG will log the error and no response will be generated.

SMG to Client APP

1. A Data Transfer Response (10304) shall be sent to the ***Destination Address*** (Client APP) field in the Service header once the message has been received from a foreign SMG and validated.
2. Client APP shall validate the ISMG signature.
   - If signature validation fails, the Client APP shall log the failure and no response shall be sent back to SMG.
   - If signature is validated, then the Client APP continues to process message.
3. The Client APP shall validate that the responding RR is a valid system user.
   - If responding RR is not a valid system user, then Client APP shall log the error and no response shall be sent back to SMG.
   - If responding RR is a valid system user, then Client APP shall continue to process message.

Client APP Validation of Data Transfer Response

1. The Client APP shall validate the Service Header fields.
   - If any of the Service Header fields are malformed, the Client APP shall log the error and no response shall be sent back.
   - If any of the Service Header fields are invalid, then the Client APP shall log the error and no response shall be sent back.

- If Service Header fields are validated, then Client APP shall continue to process message.

2. The Client APP shall validate the Service Payload fields
   - If any of the Service Payload fields are malformed, the Client APP shall log the error and no response will be sent back.
   - If any of the Service Payload fields are invalid, then the Client APP shall log the error and no response shall be sent back.
   - If the Service Payload fields are validated, then the Client APP should process the message based on the Application-to-Application behavior requirements.

Behavioral Requirements for Notification Message (10305)

Client APP to SMG

1. A Notification Message (10305) shall be generated by Client APP and sent to Domestic SMG.
2. Domestic SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the failure and no response will be sent back to Client APP.
   - If signature is validated, then Domestic SMG continues to process message.
3. The Domestic SMG shall validate the ISMG header as well as the SCAC from the ***Destination Address*** field of the Service Header.
   - If validation fails, then the SMG shall log the failure and no response will be sent back to the Client APP.
   - If the session ID within the ***Message Number*** field of the ISMG Header is something other than 0, then the SMG shall log the error and no response will be sent back to the client APP.
   - If ISMG header and SCAC are validated, then SMG continues to process message.

SMG to SMG

1. Domestic SMG shall send 10305 message to Foreign SMG.
   - If Foreign SMG is not configured in Domestic SMG, then the SMG will log the error and no response shall be sent back to Client APP.
2. Foreign SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the error and no response will be sent back to Domestic SMG.
   - If signature is validated, then Foreign SMG continues to process message.
3. Foreign SMG shall send message to EMP address in the ***Destination Address*** field in the service header.
   - If the ***Destination Address*** is an invalid EMP address, then the Foreign SMG will log the error and no response will be generated.

SMG to Client APP

1. A Notification Message (10305) shall be sent to the ***Destination Address*** (Client APP) field in the Service header once the message has been received from a foreign SMG and validated.
2. Client APP shall validate the ISMG signature.

- If signature validation fails, the Client APP shall log the failure and no response shall be sent back to SMG.
- If signature is validated, the Client APP continues to process message.

Client APP Validation of Notification Message

1. The Client APP shall validate the Service Header fields.
   - If any of the Service Header fields are malformed, then the Client APP shall log the error and shall respond with a Notification Response Message (10306) with a ***Notification Response Code*** of *"Negative Acknowledgment"* in the service payload.
   - If any of the Service Header fields are invalid, then the Client APP shall log the error and shall respond with a Notification Response Message (10306) with a ***Notification Response Code*** of *"Negative Acknowledgment"* in the service payload.
   - If Service Header fields are validated, then Client APP shall continue to process message.
2. The Client APP shall validate the Service Payload fields.
   - If any of the Service Payload fields are malformed, then the Client APP shall log the error and shall respond with a Notification Response Message (10306) with a ***Notification Response Code*** of *"Negative Acknowledgment"* in the service payload.
   - If any of the Service Payload fields are invalid, then the Client APP shall log the error and shall respond with a Notification Response Message (10306) with a ***Notification Response Code*** of *"Negative Acknowledgment"* in the service payload.
   - If the Service Payload fields are validated, then the Client APP should process the message based on the Application-to-Application behavior requirements.

Behavioral Requirements for Notification Response Message (10306)

Client APP to SMG

1. A Notification Response Message (10306) shall be generated by Client APP and sent to Domestic SMG.
2. Domestic SMG shall validate the ISMG signature.
   - If signature validation fails, the SMG shall log the failure and no response will be sent back to Client APP.
   - If signature is validated, then Domestic SMG continues to process message.
3. The Domestic SMG shall validate the ISMG header as well as the SCAC from the ***Destination Address*** field of the Service Header.
   - If validation fails, then the SMG shall log the failure and no response will be sent back to the Client APP.
   - If the session ID within the ***Message Number*** field of the ISMG Header is something other than 0, then the SMG shall log the error and no response will be sent back to the Client APP.
   - If ISMG header and SCAC are validated, then SMG continues to process message.

SMG to SMG

1. Domestic SMG shall send 10306 message to Foreign SMG.
   - If Foreign SMG is not configured in Domestic SMG, then the SMG will log the error and no response shall be sent back to Client APP.
2. Foreign SMG shall validate the ISMG signature.

- If signature validation fails, the SMG shall log the error and no response will be sent back to Domestic SMG.
- If signature is validated, then Foreign SMG continues to process message.

3. Foreign SMG shall send message to EMP address in the ***Destination Address*** field in the service header.
    - If the ***Destination Address*** is an invalid EMP address, then the Foreign SMG will log the error and no response will be generated.

SMG to Client APP

1. A Notification Response Message (10306) shall be sent to the ***Destination Address*** (Client APP) field in the Service header once the message has been received from a foreign SMG and validated.
2. Client APP shall validate the ISMG signature.
    - If signature validation fails, the Client APP shall log the failure and no response shall be sent back to SMG.
    - If signature is validated, then the Client APP continues to process message.

Client APP Validation of Notification Response Message

1. The Client APP shall validate the Service Header fields.
    - If any of the Service Header fields are malformed, then the Client APP shall log the error and no response shall be sent back.
    - If any of the Service Header fields are invalid, then the Client APP shall log the error and no response shall be sent back.
    - If Service Header fields are validated, then Client APP shall continue to process message.
2. The Client APP shall validate the Service Payload fields
    - If any of the Service Payload fields are malformed, then the Client APP shall log the error and no response will be sent back.
    - If any of the Service Payload fields are invalid, then the Client APP shall log the error and no response shall be sent back.
    - If the Service Payload fields are validated, then the Client APP should process the message based on the Application-to-Application behavior requirements.

Abbreviations and Acronyms

ACRONYMS	EXPLANATION
AAR	Association of American Railroads
AG	Advisory Group
EMP	Edge Message Protocol
FRA	Federal Railroad Administration
ISMG	Interoperable System Management Gateway
ITC	Interoperable Train Control
ITC-PTC	Interoperable Train Control-Positive Train Control
ITCSM	Interoperable Train Control System Management
ITCM	Interoperable Train Control Messaging
MAIN	Monitoring and Analysis of the Integrated Network
MAIN-CDX	Monitoring and Analysis of the Integrated Network-Core Data Exchange
MSRP	Manual of Standards and Recommended Practices
PTC	Positive Train Control
SCAC	Standard Carrier Alpha Code
SMID	System Management ID
SMG	System Management Gateway
SSO	Single Sign-On
TBC	To-Be-Configured
TTCI	Transportation Technology Center, Inc.
UAT	User Acceptance Testing