

DEPARTAMENTO DE  
**SALUD**



# Deliverable 205-ICD: ASUME Batch Participant Information: Interface Control Document (ICD)

MEDITI3G Project  
Government of Puerto Rico

**Version 3.1**  
**September 22, 2023**

**Contract # 2022-DS0707-E**

## Document Revision History

Table 1 - Document Revision History

Version Number	Date	Description
1.0	12/09/2019	Submission of the document for approval.
2.0	11/30/2020	<ul style="list-style-type: none"> <li>The following changes were made to the document:</li> <li>Updated Contract number, document version number to 2.0 and re-submission date.</li> <li>Changed throughout the document the use of "will", "should", "would", and "could" to "shall".</li> <li>Fixed table page numbers throughout the document.</li> <li>Updated Table 2: Document Approval (page iii) and Table 3: Team members (page 3), based on changes of personnel within the team and stakeholders.</li> <li>Page iv: Updated the Table of Contents to reflect the addition of the tables.</li> <li>Page 2, Section 1.1, Paragraph 1: Added Comma.</li> <li>Page 2, Section 1.1, Paragraph 1: Removed "In addition".</li> <li>Page 2, Section 1.2, Paragraph 1: Changed requests with collection of requests.</li> <li>Page 3, Section 1.3, Paragraph 1: Added paragraph.</li> <li>Page 3, Section 1.3, Paragraph 2: Added ASUME team members to the table, removed IV&amp;V members, and updated the PMO members list.</li> <li>Page 7, Section 3.1, Paragraph 2: Updated the first assumption.</li> <li>Page 7, Section 3.1, Paragraph 9: Updated the eight assumption.</li> <li>Page 9, Section 4.1, Paragraph 5: replaced the text in the bullet.</li> <li>Page 11, Section 4.2, Paragraph 5: Sentence was added.</li> <li>Page 11, Section 4.3 Paragraph 1: Updated the first sentence.</li> <li>Page 13, Section 4.3 Paragraph 6: Added cross reference to section 5.1.5.3.</li> <li>Page 16, Section 4.5, Paragraph 5: Included the PGP encryption details.</li> <li>Page 17, Section 4.5, Paragraph 3: Included the PGP encryption details.</li> <li>Page 17, Section 4.5, Paragraph 5: Included the PGP encryption details.</li> <li>Page 17, Section 4.5, Paragraph 6: Updated the last sentence for the persistence exception.</li> </ul>



Version Number	Date	Description
		<ul style="list-style-type: none"><li>• Page 17, Section 4.5, Paragraph 7: Included the PGP encryption details.</li><li>• Page 20, Section 5.1.3, Paragraph 3: Included the PGP encryption details.</li><li>• Page 20, Section 5.1.3, Paragraph 5: Included the PGP encryption details.</li><li>• Page 21, Section 5.1.3, Paragraph 8: Included the PGP encryption details. Added new step.</li><li>• Page 24, Section 5.1.5, Paragraph 1: Changed "mechanism" to "format".</li><li>• Page 24, Section 5.1.5.1, Paragraph 1: Replaced "plain text files" with "encrypted text files".</li><li>• Page 27, Section 5.1.5.3, Paragraph 1: Added the last sentence.</li><li>• Page 28, Section 5.1.5.3.1, Paragraph 1: Updated the table data groups.</li><li>• Page 54, Section 5.1.5.3.3.2: Updated the diagram.</li><li>• Page 55, Section 5.1.5.3.3.2: Eliminated StateHubError model information.</li><li>• Page 55, Section 5.1.5.3.3.2, Paragraph 1: Updated the table data groups.</li><li>• Page 74, Section 5.1.7, Paragraph 3: Included the PGP encryption details.</li><li>• Page 75, Section 6.1, Paragraph 2: Updated the schema file.</li><li>• Page 75, Section 6.2, Paragraph 2: Updated the schema file.</li><li>• Page 88, Section 11: Changed "arrangement" to "plan" in the text. Changed the word "will" for "shall".</li><li>• Page 88, Section 12, Paragraph 1: Updated the mock service file.</li><li>• Page 53, Section 5.1.5.3.3.1, Table 19: Added column "Protected Data Type".</li><li>• Page 57, Section 5.1.5.3.3.2, Table 20: Added column "Protected Data Type".</li><li>• Page 77, Section 5.1.7, Eighth Paragraph: Added paragraph 8 to include details on specific user roles with access to FTI data on the State Hub. Based on CIM comment #5 and #6 from ADSEF Real Time Participant Information ICD v2.0.</li><li>• Page 78, Section 5.1.7, Paragraph 9: Added Paragraph 9 and added Figure 8 to include details on security and release management.</li></ul>



Version Number	Date	Description
3.0	3/24/2022	<ul style="list-style-type: none"><li>• Updated Document Approval section to include Alexander Quevedo as the new stakeholder to approve technical documents.</li><li>• Updated Wovenware contact information right after Document Approval</li><li>• Updated Glossary of Terms</li><li>• Updated section 1.</li><li>• Updated section 1.1.</li><li>• Updated section 1.2.</li><li>• Updated section 1.3 Team members.</li><li>• Updated section 1.4</li><li>• Updated section 2.</li><li>• Updated section 3.1.</li><li>• Updated section 3.2.</li><li>• Updated section 3.3.</li><li>• Removed section 3.4.</li><li>• Updated section 4.1.</li><li>• Updated section 4.2.</li><li>• Updated section 4.3.</li><li>• Updated section 4.5.</li><li>• Updated section 5.1.1.</li><li>• Updated section 5.1.2.</li><li>• Updated section 5.1.3.</li><li>• Updated section 5.1.5.1.</li><li>• Updated section 5.1.5.2.</li><li>• Updated section 5.1.5.3</li><li>• Updated section 5.1.5.3.1.</li><li>• Updated section 5.1.5.3.1.1.</li><li>• Updated section 5.1.5.3.1.2.</li><li>• Updated section 5.1.5.3.1.3.</li><li>• Updated section 5.1.5.3.1.4.</li><li>• Updated section 5.1.5.3.2.</li><li>• Updated section 5.1.5.3.2.1.</li><li>• Updated section 5.1.5.3.2.2.</li><li>• Updated section 5.1.5.3.2.3.</li><li>• Updated section 5.1.5.3.3.</li><li>• Updated section 5.1.5.3.3.1.</li><li>• Updated section 5.1.5.3.3.2.</li><li>• Updated section 5.1.5.3.3.3.</li><li>• Updated section 5.1.5.3.3.</li><li>• Updated section 5.1.6.1.</li><li>• Updated section 5.1.6.2.</li></ul>



Version Number	Date	Description
		<ul style="list-style-type: none"><li>• Updated section 5.1.6.1.</li><li>• Updated section 5.1.6.2.</li><li>• Updated section 5.1.7.</li><li>• Updated section 6.1.</li><li>• Updated section 6.2.</li><li>• Updated section 7.</li><li>• Updated section 8.</li><li>• Updated section 10.</li><li>• Removed section 11 and 12.</li></ul>
<b>3.1</b>	9/22/2023	<ul style="list-style-type: none"><li>• Updated document version number to 3.1, and re-submission date.</li><li>• Page 29, Section 5.1.2, Bullet 3: Updated the bullet 3.</li><li>• Page 29, Section 5.1.2, Bullet 5: Updated the bullet 5.</li><li>• Page 33, Section 5.1.4, Paragraph 1: Updated the second sentence.</li><li>• Page 35, Section 5.1.5.2, Paragraph 1: Updated the sentence 4 and 5.</li><li>• Page 58, Section 9, Table 25: Updated the item 1.</li><li>• Page 58, Section 9, Table 25: Updated the item 2.</li></ul>

## Document Approval

Table 2 - Document Approval

Stakeholder Name	Stakeholder Role	Stakeholder Signature	Signature Date (MM/DD/YYYY)
<b>Alexander Quevedo</b>	State HIT Director		

Send inquiries to:  
**Wovenware**  
1000 Calle Los Angeles Suite 100



**San Juan, PR 00909**

**E-Mail:**

**[mediti3g@wovenware.com](mailto:mediti3g@wovenware.com)**

## Table of Contents

<b>DOCUMENT REVISION HISTORY</b>		<b>II</b>
<b>TABLE OF CONTENTS</b>		<b>VII</b>
<b>1</b>	<b>INTRODUCTION</b>	<b>10</b>
1.1	Purpose of Interface Control	10
1.2	Scope	10
1.3	Team Members	11
1.4	Glossary of Terms	12
<b>2</b>	<b>OVERVIEW</b>	<b>15</b>
<b>3</b>	<b>ASSUMPTIONS/CONSTRAINTS/RISKS/ISSUES</b>	<b>16</b>
3.1	Assumptions	16
3.2	Constraints	16
3.3	Risks and Issues	17
<b>4</b>	<b>GENERAL INTERFACE REQUIREMENTS</b>	<b>18</b>
4.1	Interface Overview	18
4.2	Functional Allocation	19
4.3	Data Transfer	20
4.4	Transactions	25
4.5	Security and Integrity	27
<b>5</b>	<b>DETAILED INTERFACE REQUIREMENTS</b>	<b>28</b>
5.1	Requirements for ASUME Batch Participant Information Interface	28
5.1.1	Assumptions	28
5.1.2	Constraints	29
5.1.3	General Processing Steps	29
5.1.4	Interface Processing Time Requirements	33
5.1.5	Message Format (or Record Layout) and Required Protocols	34
5.1.5.1	File Layout	34
5.1.5.2	Data Assembly Characteristics	35
5.1.5.3	Field/Element Definition	35
5.1.6	Communication Methods	45
5.1.6.1	Interface Initiation	46
5.1.6.2	Flow Control	47
5.1.7	Security Requirements	49
<b>6</b>	<b>XML SCHEMAS</b>	<b>50</b>
6.1	Request and Response Manifest Schemas	50
6.2	ASUME Request and Response Schemas	50



---

<b>7</b>	<b><u>QUALIFICATION METHODS</u></b>	<b>51</b>
<b>8</b>	<b><u>RELATED DOCUMENTS</u></b>	<b>52</b>
<b>9</b>	<b><u>REQUIREMENTS MATRIX</u></b>	<b>53</b>
<b>10</b>	<b><u>ISSUE REGISTER</u></b>	<b>61</b>
<b>11</b>	<b><u>APPENDIX A – ASUME API</u></b>	<b>62</b>

## **LIST OF TABLES**

Table 1 - Document Revision History	ii
Table 2 - Document Approval	v
Table 3 - Team Members	11
Table 4 - Glossary of Terms	12
Table 5 - File Naming Convention for the State Hub ZIP Files	21
Table 6 - Description of the File Naming Standards for the State Hub SFTP File Naming Conventions	22
Table 7 - ASUME Batch Participant Information Interface Processing Steps	29
Table 8 - ASUME Batch Participant Information Interface Processing Steps When the Interface Processing Ends Before Processing the Complete Batch Transaction	31
Table 9 - ASUME Batch Participant Information Interface Processing Steps to Delete Inbound File That is 14 Days or Older	32
Table 10 - ASUME Batch Participant Information Interface Processing Steps to Delete Outbound File That is 14 Days or Older	33
Table 11 - Scenarios in Cases Where the Interface Processing Ends Before Processing the Complete Batch Transaction	33
Table 12 - Request Manifest Schema: Requester to State Hub Inbound Batch File	37
Table 13 - NACK Manifest Schema: State Hub to Requester NACK file	38
Table 14 - NACK Manifest Schema: State Hub to Requester NACK Manifest ResponseCodes	39
Table 15 - NACK Manifest Schema: State Hub to Requester NACK Manifest Category Codes	39
Table 16 - Response Manifest Schema: State Hub to Requester File Response	40
Table 17 - Response Manifest Schema: State Hub to Requester ResponseCodes	41
Table 18 - Response Manifest Schema: State Hub to Requester BatchCategoryCodes	41
Table 19 - Request Data Elements: ASUME Batch Participant Information Interface to ASUME Batch System File Request	43
Table 20 - Response Data Elements: ASUME Batch System to ASUME Batch Participant Information Interface File Response	44



Table 21 - ResponseCode: ASUME Batch System LocalAgencyBatchResponseCode45	
Table 22 - ResponseCode: ASUME Batch System LocalAgencyIndividualResponse/ResponseCode	45
Table 23 - Related Documents	52
Table 24 - General Functional Requirements	53
Table 25 - Non-Functional Requirements	58
Table 26 - Issue Register	61

## **LIST OF FIGURES**

Figure 1 - ASUME Batch Participant Information Interface Enterprise Architecture	19
Figure 2 - Inbound ASUME ZIP file with batch requests	23
Figure 3 - Outbound ASUME ZIP file with responses	24
Figure 4 - Outbound ASUME Zip file with NACK	25
Figure 5 - Transaction between MEDITI3G - Local Interface - ASUME sequence	26
Figure 6 - High Level Request Manifest UML	36
Figure 7- High Level NACK Manifest UML	38
Figure 8 - High Level Response Manifest UML	40
Figure 9 - High Level ASUME Request UML	42
Figure 10 - High Level ASUME Response UML	43
Figure 11 - ASUME Batch Participant Information Interface Process Flow	47
Figure 12 - ASUME Request and Response Manifest Schema	50
Figure 13 - ASUME Request and Response File Schema	50

## 1 Introduction

The following document shall describe in detail the interaction of a Data Verification Interface hosted in the State Hub. The State Hub is the Data Hub for the MEDITI3G Initiative of the Puerto Rico Department of Health. The Child Support Administration (ASUME, in Spanish means: “Administración para el Sustento de Menores”) Batch Participant Information Interface (henceforth Local Interface) is an interface between the MEDITI3G System and the ASUME System. The MEDITI3G System shall send a batch request to the interface to gather information about the participant in ASUME System. The interface shall collect the information returned by ASUME (henceforth Local Agency) and return it to the MEDITI3G System. As part of the efforts to move forward with MEDITI3G, the Local Interface shall be part of the State Data Verification Hub (henceforth State Hub).

### 1.1 Purpose of Interface Control

This Interface Control Document (ICD) documents and tracks the information required to define the Local Interface, which establishes connection and interaction between the MEDITI3G System and the ASUME System, aiming to bridge access to critical participant information from the Local Agency through the State Hub via batch transactions. This document establishes the specifications that the Local Interface shall contain in general, the connectivity standards between the systems, the message formatting to communicate the systems, which capabilities shall be supported by the interface, and the security considerations that shall be met.

The intended audience of the Local Interface ICD is composed of all project stakeholders, including the project sponsor, senior leadership, and the project team.

### 1.2 Scope

This document describes the service interactions, assumptions, activities, constraints, process flow, and data elements for the Local Interface. The data elements that the interface shall process from the Local Agency are child support case and income reported to the agency.

The following list defines the functionalities that are within the scope of this deliverable:

- The MEDITI3G System shall submit the PRMP participant information collection of requests to be processed by the Local Interface to look up the information in the ASUME System via batch transactions.
- The interface shall convert the responses to the standard format.
- Request and response schema validations shall be done by the Local Interface. All specified/provided rules are explained in detail in section 5: Detailed Interface Requirements.
- Log Local Interface audit trail.
- Errors shall be classified as system or data errors and shall be logged independently within the Local Interface for reference purposes.

System errors are those related (but not limited) to (1) an unexpected error while the interface processes the requested file.

Data errors are those that occurred while enforcing the data validation rules described in section 5: Detailed Interface Requirements.

The Local Interface shall be MARS-E and HIPAA compliant. Security measures shall be performed to follow PRDoH security standards and procedures. To comply with security guideline rules, all extracted data shall be handled in the State Hub internal network and shall not be transmitted outside the network while being processed. The requests and responses shall not be persisted in the State Hub, except for the files that are not processed within 14 days.

### 1.3 Team Members

The following team members shall provide their feedback for this document.

*Table 3 - Team Members*

Participants	Organization
José Falero	ASUME
Alba L. Álvarez	ASUME
Jean Beaty	PMO
Blake Hansard	PMO



Participants	Organization
Alexander Quevedo	PRMP
Irma Avilés	PRMP
Evelyn Santos	PRMP
Iván Imbert	PRMP
Ryon Johnson	Redmane
Stephanie Nieves	Redmane
Brandon Peclyak	Redmane
Tamera Jones	Redmane

## 1.4 Glossary of Terms

Table 4 - Glossary of Terms

Acronym/Term	Definition
<b>ASUME</b>	Child Support Administration. In Spanish means: "Administración para el Sustento de Menores"
<b>CMS</b>	Centers for Medicare & Medicaid Services
<b>DOB</b>	Date of Birth
<b>EFT</b>	Electronic File Transfer
<b>FTI</b>	Federal Tax Information
<b>FUNC</b>	Function
<b>GB</b>	Gigabyte
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>HIT</b>	Health Information Technology
<b>HTTPS</b>	Hypertext Transfer Protocol Secure



<b>Acronym/Term</b>	<b>Definition</b>
<b>ICD</b>	Interface Control Document
<b>IRS</b>	Internal Revenue Service
<b>IV&amp;V</b>	Independent Verification & Validation
<b>KB</b>	Knowledge Base (usually referred to Microsoft issued patches)
<b>MARS-E</b>	Minimum Acceptable Risk Standards for Exchanges
<b>MEDITI3G</b>	Medicaid Integrated Technology Initiative 3 <sup>rd</sup> Generation
<b>MOU</b>	Memorandum of Understanding
<b>NACK</b>	Negative Acknowledgment (NACK) files are the way the Local Interface will transmit to the Requestor System that an error occurred
<b>NIEM</b>	National Information Exchange Model
<b>PHI</b>	Protected Health Information
<b>PII</b>	Personally Identifiable Information
<b>PMO</b>	Project Management Office
<b>PRDoH</b>	Puerto Rico Department of Health
<b>PREE</b>	Puerto Rico Eligibility and Enrollment
<b>Requestor System</b>	Name to identify the solution used by the PRMP case workers for eligibility management.
<b>PRMP</b>	Puerto Rico Medicaid Program
<b>Requester</b>	Administrator, auditor, or consumer of service providers
<b>RSA</b>	Rivest-Shamir-Adleman Cryptosystem
<b>SHA</b>	Secure Hash Algorithm
<b>SFTP</b>	Secure File Transfer Protocol
<b>SI</b>	System Integrator
<b>SOAP</b>	Simple Object Access Protocol
<b>SSH</b>	Secure Shell
<b>SSN</b>	Social Security Number
<b>TDS</b>	Trusted Data Source
<b>TLS</b>	Transport Layer Security



<b>Acronym/Term</b>	<b>Definition</b>
<b>UML</b>	Unified Modeling Language
<b>VPN</b>	Virtual Private Network
<b>XML</b>	Extensible Markup Language

## 2 Overview

ASUME is the Local Agency in Puerto Rico responsible for the implementation of the public policy on child support and the Program of Support for the Elderly in Puerto Rico.

The Requestor System, through these batch requests, shall query the Local Interface for information regarding an applicant's/beneficiary's information in a Local Agency. The batch requests shall contain an applicant's/beneficiary's basic personally identifiable information. The Local Interface shall interact with the Local Agency to find the information in their system and return it to the Requestor System.

This solution establishes that the Local Interface is implemented as core components of the State Hub in an Azure Government environment to guarantee high availability, redundancy, data integrity, and data security using the HIPAA Privacy Rule, HIPAA Security Rule, and CMS Standards and Conditions as the basis.

## 3 Assumptions/Constraints/Risks/Issues

Several factors influence the expectations of the Local Interface. They have been categorized as assumptions, constraints, and risks.

### 3.1 Assumptions

The following assumptions apply to the ASUME Batch Interface:

1. There shall be a signed Memorandum of Understanding (MOU) agreement in place with ASUME to allow the sharing of ASUME System information.

The Requestor System shall use the interface to assist Medicaid in determining the renewal eligibility of PRMP participants.

2. The Local Agency shall promptly notify PRDoH and Wovenware the identified MEDITI3G operational personnel of any maintenance window not previously scheduled or agreed upon.

The Local Agency shall have maintenance windows at least one or two times a month during the weekends.

3. Azure Government cloud shall maintain backward compatibility for up to three (3) versions allowing enough time to update code for new offerings of services and components. The inclusion of new offerings later shall not negatively impact compatibility and compliance with HIPAA and MARS-E.

The identified MEDITI3G key personnel shall establish the necessary procedures to grant access to the SFTP Server.

4. ASUME shall provide an environment replica that shall be hosted in Azure Government.
5. The data in environment shall be replicated daily with the most recent data.

### 3.2 Constraints

This section defines limitations, such as external dependencies, identified during the interfaces' requirements gathering.

1. The interface shall be dedicated to communicating to a single Trusted Data Source (TDS) for requesting data.



2. The State Hub, the environment that shall contain the Local Interface, shall not manage files greater than 100 Gigabytes (GB).
3. The Federal Hub implements NIEM 2.0 and has not indicated when they would upgrade. Since newer versions are not backward compatible with older versions, the State Hub and the Local Interfaces shall also use NIEM 2.0.
4. ASUME does not provide the means to process a batch file request.
5. ASUME shall not share data that originated from a federal agency, such as the Federal Parent Locator Service, henceforth FPLS.

### **3.3 Risks and Issues**

No risks nor issues are currently open in the project's SharePoint site: [PREE DDI - Home \(sharepoint.com\)](#)

## 4 General Interface Requirements

This section describes the general functional decomposition of the Local Interface used by Requestor System when requesting a participant's information from ASUME's System. In addition, it shall cover the security and integrity requirements needed for the request to be considered successful and achievable.

### 4.1 Interface Overview

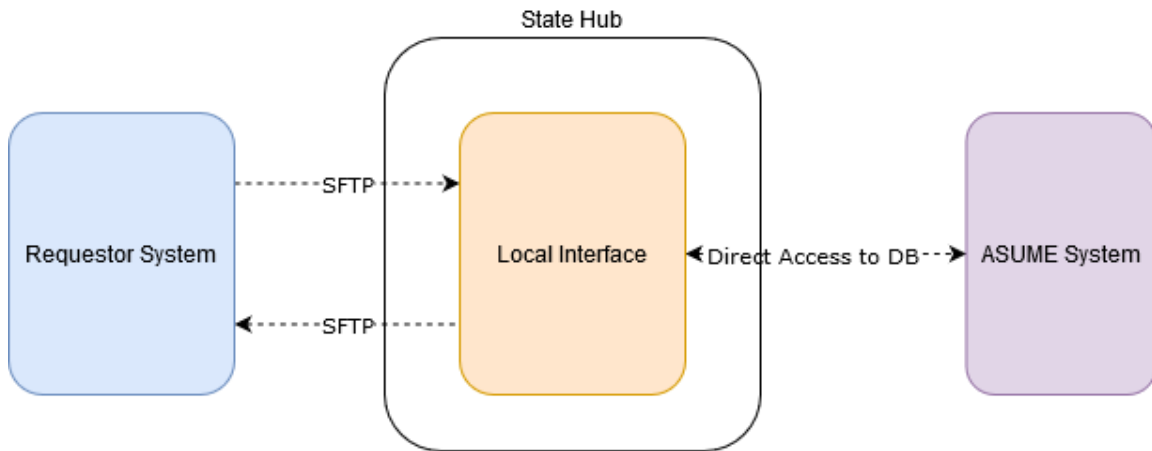
The Local Interface residing in the State Hub shall connect the Requestor System with the ASUME System seeking to acquire beneficiaries' personal information in an Application-to-Application asynchronous behavior.

The Requestor System shall generate batch interface request file(s) and send it through SFTP to the Local Interface. Multiple ZIP files are allowed to be sent to the interface for batch processing. The batch request file contains individual requests with beneficiaries' personal identifiable information that can be used to locate the participant's information within the agency's system, information such as SSN, Name, and Date of Birth (DOB).

- The interface shall validate the received file and then query the individual requests securely against the Local Agency.
- Upon locating a participant, the agency shall respond with the participant's personal information, address, child support case information, and income reported to the agency.
- Once the responses have been received from the agency, the interface will pack the response(s) in a ZIP folder and pass through to Requestor System via the State Hub SFTP Server.
- Alternatively, the interface shall determine instead to return a negative acknowledgement (NACK) back to Requestor System in the scenarios where the interface cannot process the submitted batch request file, scenarios such as when the batch request file fails validation.
- Finally, Requestor System shall be able to retrieve and delete the response from the Local Interface via SFTP.

Figure 1 - ASUME Batch Participant Information Interface Enterprise Architecture illustrates a high-level view of the interaction between the Requestor System, the Local Interface and ASUME.

*Figure 1 - ASUME Batch Participant Information Interface Enterprise Architecture*



In Figure 1, the Requestor System is the entity in charge of initiating the batch request via SFTP with the Local Interface. The ASUME System is the Local Agency system that the Local Interface shall interact with to request applicants/beneficiary’s information. The Local Interface is hosted in the State Hub and shall connect with the ASUME System via direct access to a database to perform the requests sent by the Requestor System and deliver the responses back to the Requestor System.

## 4.2 Functional Allocation

The interaction between the Requestor System and the Local Interface is triggered when the Requestor System deposits the batch request file in the inbound folder. A mechanism shall be activated when a file is deposited. As a result of this trigger, the Local Interface shall commence the business operation to process the requests against the ASUME System to gather the participant information. The process is compliant with the Patient Protection and Affordable Care Act of 2010, Section 1561. The schema that the requests shall contain are detailed in section 5.1.5 Message Format (or Record Layout) and Required Protocols.

The business operation to process the requests against the ASUME System to gather the participant information shall end before processing the complete batch transaction if one of the following conditions is met:

The interface has reached the maximum response time,

The interface has started to receive sequential errors in the responses from the Local Agency and the quantity of those errors exceed 20% of the complete batch, or

The interface losses connection to the Local Agency during a batch transaction and the connection is not established within twenty-four (24) hours.

Shall it end by one of these conditions, the interface collects the partial responses to the batch request, along with the unprocessed requests, and sends them to the Requestor System. If there are no partial responses available, the interface shall return a NACK file.

The interface shall monitor the request files left in the Inbound folder and if a batch request file is left in the Inbound folder for more than fourteen (14) days then a business process shall take place to remove the file.

The interface shall monitor the response files left in the Outbound folder and if a response file is left in the Outbound folder for more than fourteen (14) days then a business process shall take place to remove the file.

The High-Level Design Document for this interface shall further describe this business process in detail.

### **4.3 Data Transfer**

The Requestor System requests information from the ASUME System through the State Hub by placing an encrypted ZIP file containing a manifest file and the requests in XML format for the agency in the established SFTP folder. The interface shall validate the XML files against the National Information Exchange Model (NIEM) standards. Authentication and authorization details for the SFTP folder are discussed in Section 4.5.

Table 5 - File Naming Convention for the State Hub ZIP File describe the file naming conventions, attributes of the compressed ZIP file, and the folder name where the Requestor System shall place each request file to be processed against the ASUME System.

The function (**FUNC**) attribute (see Table 6 - Description of the File Naming Standards for the State Hub SFTP File Naming Conventions) for the ASUME Batch Participant Information Interface is **ASUMBPII**.

*Table 5 - File Naming Convention for the State Hub ZIP File*

SFTP Folder	Filename
<b>Inbound folder</b> <b>For Inbound (Requester to State Hub)</b>	SOURCEID.FUNC.DATE.TIME.ENV.IN e.g., MEDITI3G.ASUMEBPII.D191114.T065423325.T.IN
<b>Outbound (Response) Folder</b> <b>For NACK (State Hub to Requester)</b>	SOURCEID.FUNC.DATE.TIME.ENV.OUT e.g., MEDITI3G.NAK.D191114.T065423325.T.OUT
<b>Outbound (Response) Folder</b> <b>For Response (State Hub to Requester)</b>	SOURCEID.FUNC.DATE.TIME.ENV.OUT e.g., MEDITI3G.OUT.D191114.T065423325.T.OUT

Table 6 - Description of the File Naming Standards for the State Hub SFTP File Naming Conventions defines the specific information for each attribute in the Inbound and Outbound State Hub SFTP ZIP filenames.

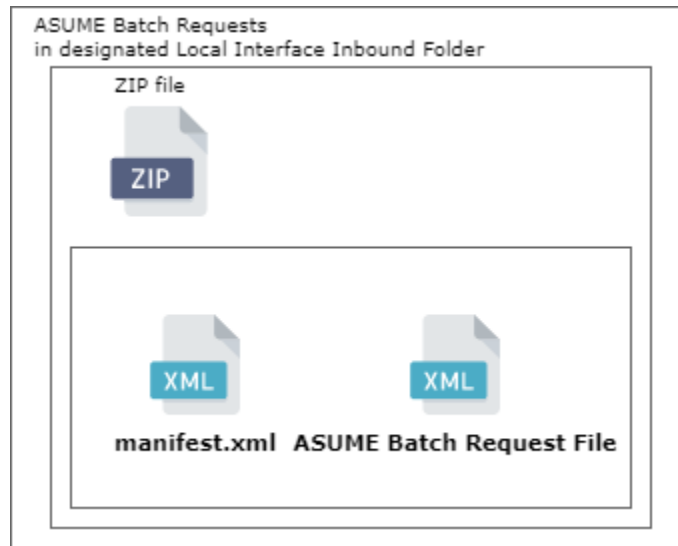
*Table 6 - Description of the File Naming Standards for the State Hub SFTP File Naming Conventions*

Attribute	Description
<b>SourceID</b>	The source identification given to the Requestor to identify State Hub request match file.
<b>Func</b>	The specific data function that is requested to the State Hub.
<b>Date</b>	The date of the file submitted identified by the following format DYYMMDD
<b>Time</b>	The timestamp of the file submitted identified by the following format THHMMSSNNN (if milliseconds are not available, any three digits shall be used, as long as the resultant filename is unique)
<b>Env</b>	The environment in which the file is being submitted (P for Production Environment (PROD), T for non-PROD)
<b>In</b>	File extension mandated for files Inbound to Electronic File Transfer (EFT) Note: This is only applicable for the Inbound folder.
<b>Out</b>	Transfer direction Note: This is only applicable for the Outbound folder.

Section 5.1.5.3 Field/Element Definition contains a description of the schema each XML file must contain in order to pass validations and be routed to the ASUME System.

Figure 2 - Inbound ASUME ZIP file with batch requests illustrates a batch request in the designated Local Interface Inbound folder with one manifest and one ASUME batch request file. The manifest file contains metadata information about the files within the ZIP file. See section 5.1.5.3 Field/Element Definition for more details.

Figure 2 - Inbound ASUME ZIP file with batch requests

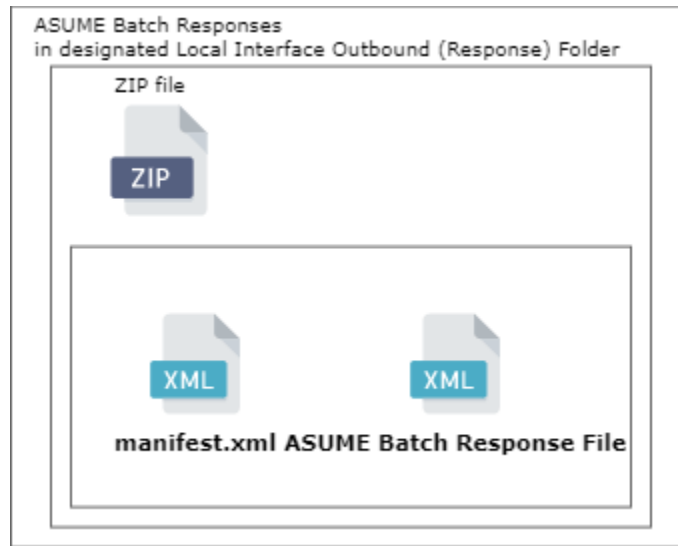


The interface shall request the information from ASUME using secure connection to the database provided by TLS. The requests sent and the responses received from the database are processed in XML format.

After the interface has received in XML format the response(s) from the ASUME System, a response file and a manifest file are created in XML format following NIEM standards, the resulting files are compressed into a ZIP file and uploaded to the established SFTP folder for Requestor System to download them.

Figure 3 - Outbound ASUME ZIP file with responses illustrates a batch response in the designated Local Interface Outbound folder with one manifest and one ASUME batch response file.

Figure 3 - Outbound ASUME ZIP file with responses

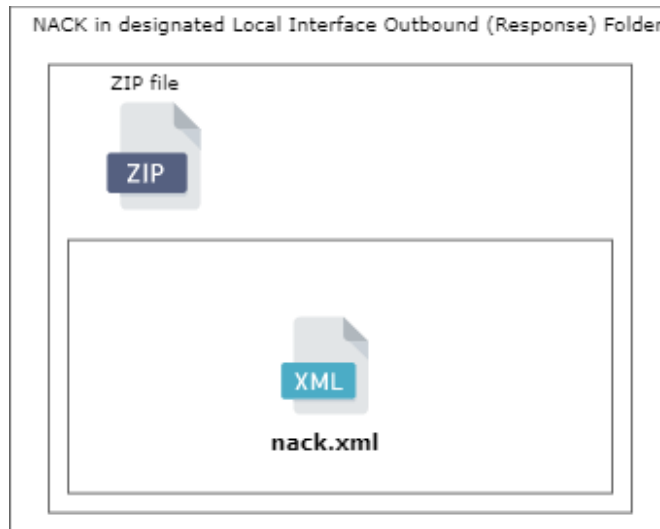


When a validation error of the whole batch request file has occurred at the TDS, the TDS shall create and return to the interface a NACK file containing information about the batch that generated the error and an error code to identify the type of error. The interface shall prepare and send a NACK file to the Requestor System.

Figure 4 - Outbound ASUME Zip file with NACK illustrates a NACK in the designated Outbound folder with one manifest. A NACK only contains one manifest file within the ZIP file.



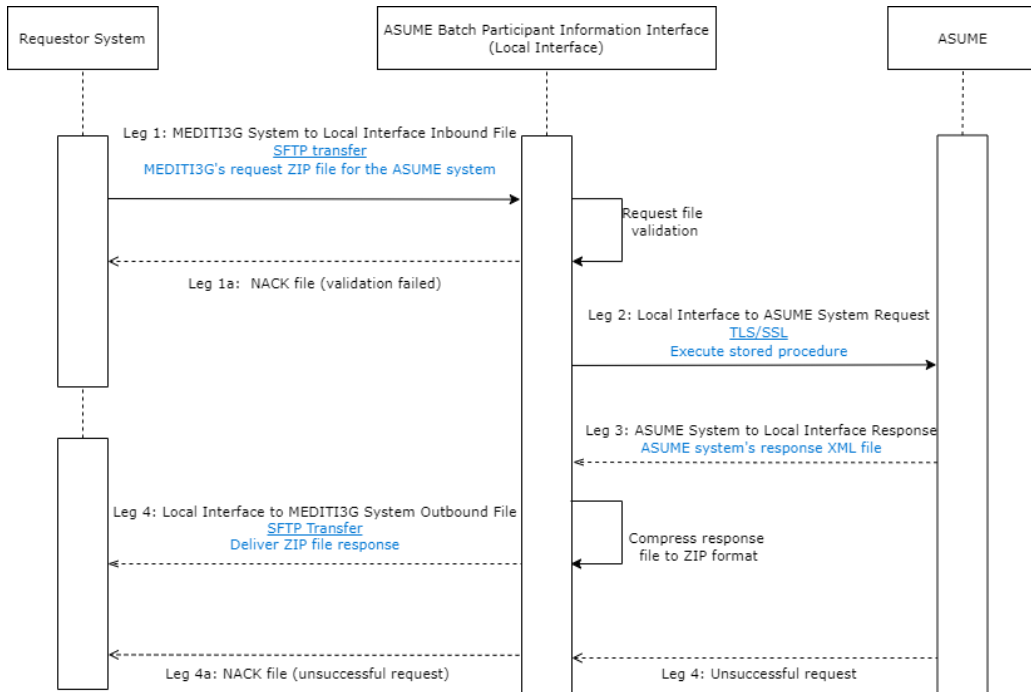
*Figure 4 - Outbound ASUME Zip file with NACK*



## 4.4 Transactions

The batch request file transaction between Requestor System and ASUME System is described below:

*Figure 5 - Transaction between MEDITI3G - Local Interface - ASUME sequence*



**Leg 1: Requestor System to Local Interface Inbound File**

- The ASUME Batch Participant Information Interface shall receive the transaction. This transaction includes requests with personally identifiable information such as Full Name, SSN and DOB.

**Leg 1a: NACK File (validation failed)**

- The interface shall generate a NACK file if a validation occurs with the request received.

**Leg 2: Local Interface to ASUME System Request.**

- The interface shall process the batch requests against the ASUME system via a Stored Procedure. The query information shall be sent to the Stored Procedure in XML format. This transaction shall send the requests from Leg 1 to the ASUME System.

**Leg 3: ASUME System to Local Interface Response**

- The interface is responsible for receiving and validating the responses from the stored procedure in XML format following NIEM standards. This transaction includes the responses from the ASUME System containing `` personally

identifiable information, child support case information and the reported income to the agency.

#### Leg 4: Local Interface to Requestor System Outbound File

- A manifest file is created for the response file. Both files are compressed in ZIP format. The final ZIP response file is delivered to the Requestor System via SFTP. This transaction shall take the responses from Leg 3 and deliver them to the Requestor System.

#### Leg 4a: NACK file (unsuccessful request)

- The interface shall generate a NACK file if unsuccessful request error was received from the local agency.

## 4.5 Security and Integrity

The processed request shall be used as part as the stored procedure call used to access ASUME's provided data. The stored procedure call shall be done using secured channels and a VPN. Processed request data shall be encrypted while in transit to ASUME. Since data shall be obtained and returned to the State Hub using the same channel, the same security considerations shall be applied. The Local Interface shall encrypt the response file using PGP, before returning the file to the Requestor. Similarly, all security enforced during the request processing shall be applied to the data returned from ASUME to the SFTP where the Requestor System shall collect it.

## 5 Detailed Interface Requirements

The following section provides a detailed description of the interaction between the Requestor System and the ASUME System through the Local Interface in the State Hub.

### 5.1 Requirements for ASUME Batch Participant Information Interface

This ASUME Batch Participant Information interface shall be used to transfer a matched request file from the Requestor System to ASUME and back. Full details on this end-to-end process, the requirements that it shall meet, any assumptions that have been made and constraints that have been identified are outlined in the below sections.

#### 5.1.1 Assumptions

The following assumptions are considered for the design of this interface:

- ASUME and the Local Interface shall connect via a VPN Tunnel.
- The ASUME Batch Participant Information Interface shall interact with ASUME through a stored procedure that resides in ASUME's side, as agreed with the agency.
- The ASUME Batch Environment shall be available 24 hours a day, 7 days a week. Except any previously maintenance scheduled or agreed upon.
- ASUME's network shall need to be configured as to accept a large amount of concurrent connections.
- The ASUME Batch Environment shall have a scheduled downtime due to the replication process.
- The replication process is expected to be incremental.
- The Local Agency shall promptly notify PRMP of any maintenance window not previously scheduled or agreed upon.
- The interface shall only have access to execute the Stored Procedure in the TDS database.

- The TDS shall support up to 1,000 individual requests on a single call.
- The TDS response shall include replicated timestamp.

### 5.1.2 Constraints

The following constraints apply to the interactions between the Requestor System and the Local Interface:

- The Local Interface shall perform matches based on the following combinations:
  - SSN
  - First Name and Last Name (paternal)
  - Date of Birth (DOB)
- The maximum response time for batch, shall be five (5) calendar days.
- The batch local interfaces shall only process up to one (1) request file at a time.
- Each batch request shall have its own ZIP file.
- The XML request file within the ZIP file shall not be greater than 250MB.
- The Federal Hub implements NIEM 2.0 and has not indicated if and when they would upgrade. Since newer versions are not backward compatible with older versions, the State Hub and the Local Interfaces shall also use NIEM 2.0.

### 5.1.3 General Processing Steps

Table 7 - ASUME Batch Participant Information Interface Processing Steps details the processing steps that the interface completes monthly to process the requests from the Requestor System to the ASUME Batch Participant Information Interface.

*Table 7 - ASUME Batch Participant Information Interface Processing Steps*

Processing Step	Description	Responsible
<b>1</b>	The Requestor System deposits the PGP encrypted ZIP file containing the batch requests to the ASUME System in the State Hub SFTP server.	MEDITI3G

Processing Step	Description	Responsible
2	The SFTP server encrypts the file right after the upload is completed.	Local Interface
3	The interface shall detect the new deposited file in the SFTP and decrypt the file using the PGP private key.	Local Interface
4	The decrypted ZIP file is decompressed.	Local Interface
5	The manifest file is read and validated, as well as the ASUME request file. If the interface detects an error in validation a NACK file is sent to the Requestor System.	Local Interface
6	The ASUME batch request file is an XML 1.0 format file. It is validated with NIEM 2.0 standards. If the file does not meet the NIEM 2.0 Standards the interface sends a NACK file to the Requestor System.	Local Interface
7	<p>The Local Interface shall check if the Local Agency System is available. If the connection to the Local Agency is not established within twenty-four (24) hours, the local interface shall stop the batch transaction and the partial results available are returned. If there no partial results available, a NACK file is returned.</p> <p>When this is triggered, the process that follows is detailed in Table 8 - ASUME Batch Participant Information Interface Processing Steps When the Interface Processing Ends Before Processing the Complete Batch Transaction.</p>	Local Interface
8	The validated ASUME requests are segmented into groups of thousand (1,000) and sent to the local agency system.	Local Interface
9	<p>If the Local Interface receives 20% (of the complete batch) or more sequential errors, or reaches the maximum response time, the batch transaction is stopped and the partial results available are returned. If there no partial results available, a NACK file is sent.</p> <p>When this is triggered, the process that follows is detailed in Table 8 - ASUME Batch Participant Information Interface</p>	Local Interface

Processing Step	Description	Responsible
	Processing Steps When the Interface Processing Ends Before Processing the Complete Batch Transaction.	
<b>10</b>	The responses are collected until all the requests has been made to the local agency system and the responses has been received.	Local Interface
<b>11</b>	The responses received in XML format from the ASUME System are validated to be XML 1.0 format following NIEM 2.0 standards.	Local Interface
<b>12</b>	The response manifest file is generated, and the files are compressed.	Local Interface
<b>13</b>	The compressed file is encrypted with PGP.	Local Interface
<b>14</b>	The resulting file is placed in the State Hub SFTP Outbound folder where the file is encrypted while the file is at rest in the server.	Local Interface
<b>15</b>	The Requestor System retrieves and deletes the response file from the Outbound SFTP folder.	MEDITI3G

Table 8 - ASUME Batch Participant Information Interface Processing Steps When the Interface Processing Ends Before Processing the Complete Batch Transaction details the processing steps that the interface completes when the Local Interface receives 20% or more sequential errors on the complete batch, the maximum response time has been reached or connection to the Local Agency was not established within twenty-four (24) hours.

*Table 8 - ASUME Batch Participant Information Interface Processing Steps When the Interface Processing Ends Before Processing the Complete Batch Transaction*

Processing Step	Description	Responsible
<b>1</b>	The interface receives 20% or more sequential errors on the complete batch, the maximum response time has been	Local Interface

Processing Step	Description	Responsible
	reached or connection to the Local Agency was not established within twenty-four (24) hours.	
<b>2</b>	Verify if there have been partial responses collected during the execution.	Local Interface
<b>3</b>	If partial responses have been collected, create a manifest file with the partial responses and place them in the State Hub SFTP Outbound folder.	Local Interface
<b>4</b>	If no partial responses have been collected, create a NACK response and place it in the State Hub SFTP Outbound folder.	Local Interface

Table 9 - ASUME Batch Participant Information Interface Processing Steps to Delete Inbound File That is 14 Days or Older details the processing steps that the interface completes to delete any file that is fourteen (14) days or older in the Inbound folder.

*Table 9 - ASUME Batch Participant Information Interface Processing Steps to Delete Inbound File That is 14 Days or Older*

Processing Step	Description	Responsible
<b>1</b>	The interface monitors the Inbound folder.	Local Interface
<b>2</b>	Verify the date that the file was placed in the folder.	Local Interface
<b>3</b>	Delete the file if it is ten (14) days or older.	Local Interface

Table 10 - ASUME Batch Participant Information Interface Processing Steps to Delete Outbound File That is 14 Days or Older details the processing steps that the interface completes to delete any file that is fourteen (14) days or older in the Outbound folder.



*Table 10 - ASUME Batch Participant Information Interface Processing Steps to Delete Outbound File That is 14 Days or Older*

Processing Step	Description	Responsible
1	The interface monitors the Outbound folder.	Local Interface
2	Verify the date that the file was placed in the folder.	Local Interface
3	Delete the file if it is ten (14) days or older.	Local Interface

### 5.1.4 Interface Processing Time Requirements

The minimum response time of the batch file shall be within one (1) day with a maximum response time of nine (9) calendar days. This maximum response time considers that the number of compressed files queued for processing shall be one (1).

Table 11 - In cases where the interface processing ends before processing the complete batch transaction, the response file shall vary as presented in this table. Cases such as exceeded the maximum response time, 20% or more sequential errors where received from the complete batch transaction, or the interface was not able to communicate with the Local Agency within twenty-four (24) hours.

*Table 11 - Scenarios in Cases Where the Interface Processing Ends Before Processing the Complete Batch Transaction*

Processing State Scenarios	Result
<b>The ASUME Batch Participant Information Interface has obtained a partial response from the ASUME System.</b>	A response with partial responses containing the partial data it has at moment and for every un-processed individual request the response shall contain an error code.

Processing State Scenarios	Result
Example: the interface has been able to process a certain number of requests, but the maximum response time was reached.	
<p><b>The ASUME Batch Participant Information Interface has not received a response from the ASUME System.</b></p> <p>Example: the interface has not been able to process any requests against the ASUME System.</p>	The response shall be a NACK file.

All the results in these cases shall be audited and presented in audit reports concerning exceeded response time.

In the case where connections are not being made to the ASUME data store, the State Hub shall continue to make requests every thirty (30) minutes up to the five (5) calendar days of the response time, or twenty-four (24) hours of continuous failed attempts.

### 5.1.5 Message Format (or Record Layout) and Required Protocols

The following section shall detail the format by which the Requestor System shall send participant batch requests to ASUME and ASUME shall respond to the requests sent by the Requestor System.

#### 5.1.5.1 File Layout

The ASUME Batch request and response files are encrypted text files in XML format following NIEM standards. Each batch request file sent by the Requestor System shall follow the file format defined in section 0:

Field/Element Definition.

### 5.1.5.2 Data Assembly Characteristics

The data that is processed in the interface is in XML format following NIEM standards version 2.0. The manifest file shall include detailed information about the batch transaction being sent to the ASUME. The manifest file contains information such as the number of files sent in the batch, the number of requests being made to ADSEF, the checksum of the files, and the name of the files within the ZIP file. The maximum file size limit for ASUME request files inside the ZIP file is 262,144,000 bytes (250 megabytes). In terms of individual requests, a single 250 MB request file can hold up to three hundred thousand (300,000) individual requests. The request file can be split up into multiple request files in the case where they exceed this specified file size.

The request file contains one or more individual requests to the ASUME System with information about the participant that is going to be matched. The individual request includes a batch identifier, a request identifier, the name of the participant, the date of birth and the social security number. On the other hand, the response file created to the Requestor System includes one or more individual responses about the participant and the identifier for each request. Each participant's record returns the personal information stored, address(es), income reported and data about the child support case.

The NACK file shall inform of any file validation errors encountered in the process and the batch that failed the validation. If any request, attachment, or manifest file in the ZIP has a validation error, it shall also be specified in the file. The NACK shall also return any error found during schema validation as well as any error captured during the processing of the match request file against the ASUME System.

The ASUME Batch Participant Information Interface file layouts are defined in section 0:

Field/Element Definition.

### 5.1.5.3 Field/Element Definition

The following section details the schema used between the Requestor System and the Local Interface to request participant information from the Local Agency. This section also provides details for error encountered during the transactions and how the error is reported back to the Requestor System. Section 6 provides a sample schema and sample XML for the data elements in the following section.

#### 5.1.5.3.1 Batch Service Request Manifest Data Elements, NACK Manifest ResponseCodes, and BatchCategoryCodes

The following section shall detail the manifest request schema by which the Requestor System shall send the batch request to the Local Agency, the NACK elements that shall be sent to the Requestor System if any error was encountered while validating the requests and the error codes that shall be used to inform the Requestor System of the error encountered.

##### 5.1.5.3.1.1 Request Manifest Data Elements

The Requestor System that sends batch data verification request to the Local Interface shall populate the request manifest schema to describe the files the Requester is submitting to the State Hub. The name of the request manifest file is manifest.xml.

Figure 6 - High Level Request Manifest UML illustrates the elements that the manifest request shall contain submit the requests to the Local Interface. Detailed data elements are described in Table 12 - Request Manifest Schema: Requester to State Hub Inbound Batch File.

*Figure 6 - High Level Request Manifest UML*

### Request Manifest

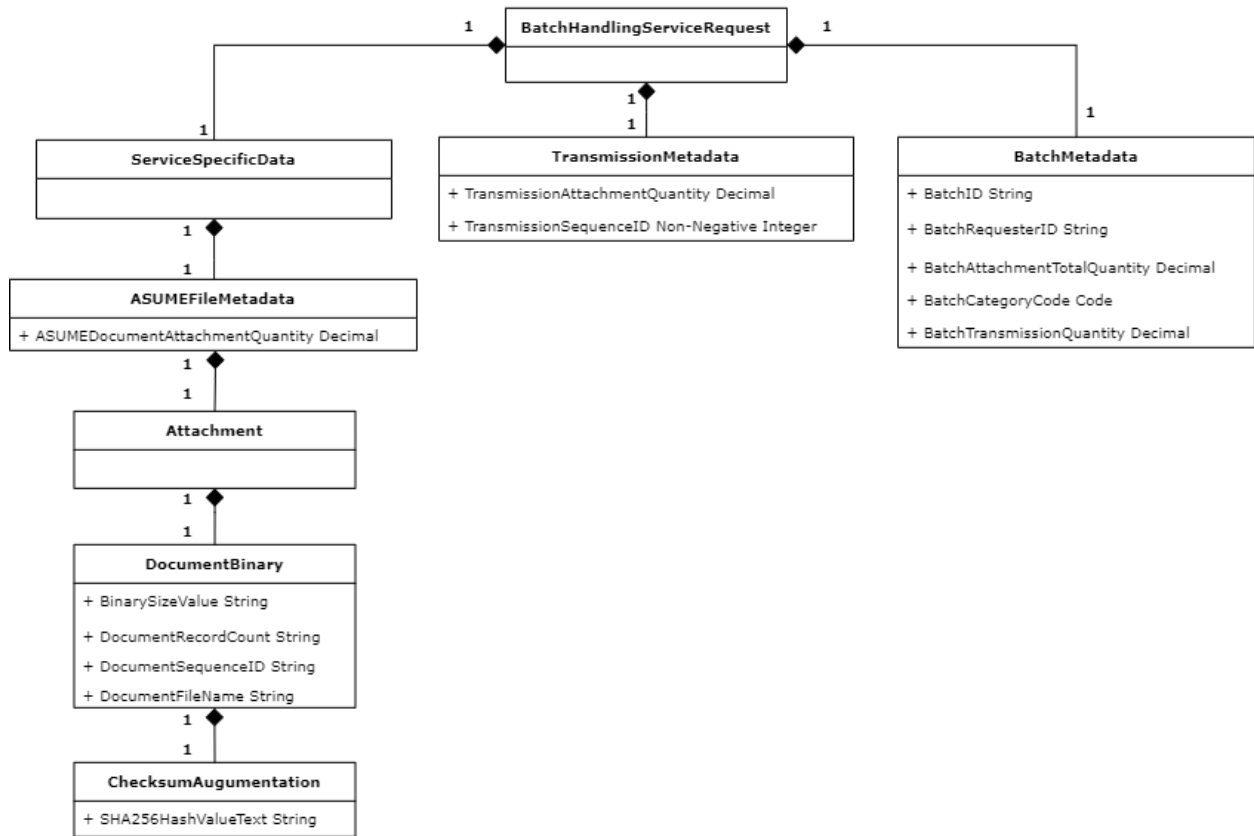


Table 12 - Request Manifest Schema: Requester to State Hub Inbound Batch File defines the data elements that the request manifest needs for a batch request to be submitted to the Local Interface. The following data elements define the attributes of the TDS-destined file the Requester need to submit to the State Hub.

*Table 12 - Request Manifest Schema: Requester to State Hub Inbound Batch File*



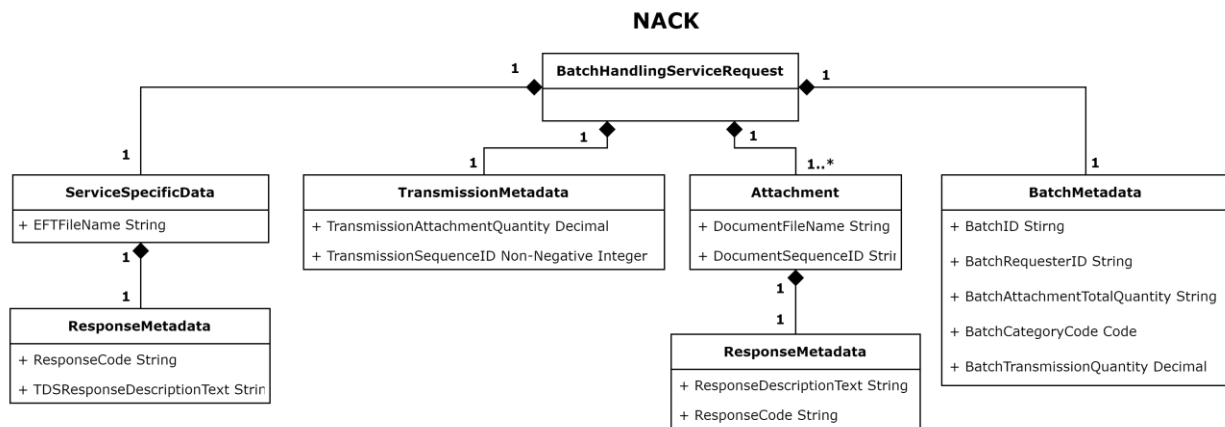
Request Manifest  
Schema.xlsx

5.1.5.3.1.2 NACK Data Elements

Table 13 - NACK Manifest Schema: State Hub to Requester NACK file defines the data elements that the State Hub NACK file returns to the Requester when an error in validation or during the process was encountered. The detailed information of the errors that are sent in the NACK file is found in section 5.1.5.3.1.3: NACK Manifest ResponseCodes. The following data elements define the attributes of the NACK file that the State Hub returns to the Requester when an error has occurred.

Figure 7- High Level NACK Manifest UML illustrates the elements that the NACK response shall contain to receive the NACK from the Local Interface. Detailed data elements are described in Table 13 - NACK Manifest Schema: State Hub to Requester NACK file.

*Figure 7- High Level NACK Manifest UML*



*Table 13 - NACK Manifest Schema: State Hub to Requester NACK file*



NACK Manifest  
Schema.xlsx

### 5.1.5.3.1.3 NACK Manifest ResponseCodes

Table 14 – NACK Manifest Schema: State Hub to Requester NACK Manifest ResponseCodes defines the NACK Manifest response codes that the State Hub return to the Requester when an error in validation or during the process where encountered. The following data elements define the attributes of the NACK Manifest ResponseCodes that the State Hub returns to the Requester when an error has occurred.

*Table 14 - NACK Manifest Schema: State Hub to Requester NACK Manifest ResponseCodes*



NACK Manifest  
Response Codes.xlsx

### 5.1.5.3.1.4 NACK Batch Category Codes

Table 15 - NACK Manifest Schema: State Hub to Requester NACK Manifest Category Codes defines the NACK Manifest Category Codes that the State Hub returns to the Requester when an error in validation or during the process where encountered. The following data elements define the attributes of the NACK Manifest Category Codes that the State Hub return to the Requester when an error has occurred.

*Table 15 - NACK Manifest Schema: State Hub to Requester NACK Manifest Category Codes*



NACK Manifest  
Category Codes.xlsx

### 5.1.5.3.2 Batch Service Response Manifest Data Elements, ResponseCodes and BatchCategoryCodes

The following section shall detail the manifest response schema by which the Local Interface shall send the response to the Requestor System and the error codes that shall be used to inform the Requestor System of the error encountered.

5.1.5.3.2.1 *Response Manifest Data Elements*

The State Hub populates the response manifest schema to return responses from the TDS to Requesters. The response manifest filename is manifest.xml.

Figure 8 - High Level Response Manifest UML illustrates the elements that the manifest response shall contain to receive the responses from the Local Interface. Detailed data elements are described in Table 16 - Response Manifest Schema: State Hub to Requester File Response.

*Figure 8 - High Level Response Manifest UML*

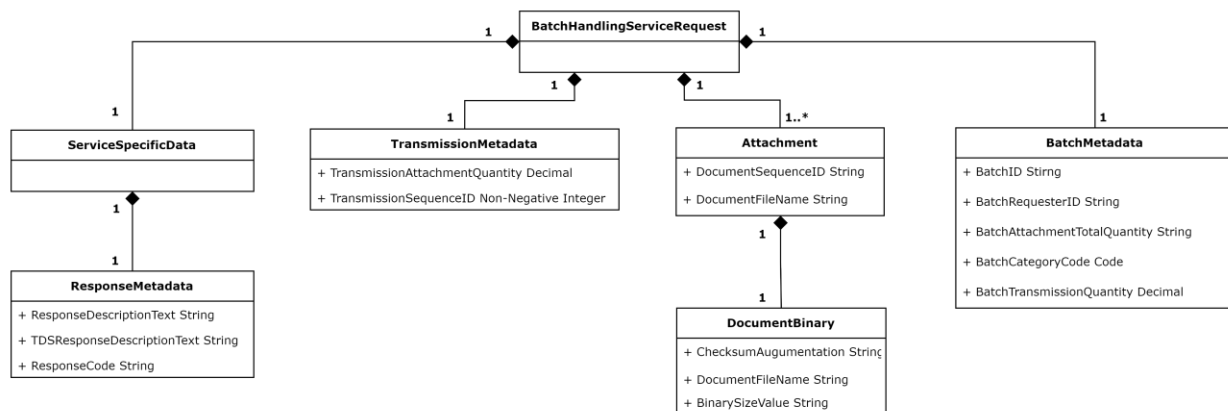


Table 16 - Response Manifest Schema: State Hub to Requester File Response defines the response data elements that the State hub needs to return to the Requester. The following data elements define the attributes of the file that the State hub return to the Requester.

*Table 16 - Response Manifest Schema: State Hub to Requester File Response*



5.1.5.3.2.2 *Response Manifest File-level ResponseCodes*



Table 17 – Response Manifest Schema: State Hub to Requester ResponseCodes defines Manifest File response codes that the State Hub return to the Requester. The following data elements define the attributes of the Manifest ResponseCodes that the State Hub return to the Requester when an error has occurred.

*Table 17 - Response Manifest Schema: State Hub to Requester ResponseCodes*



Response Manifest  
Response Codes.xlsx

#### *5.1.5.3.2.3 Response Manifest BatchCategoryCodes*

Table 18 – Response Manifest Schema: State Hub to Requester BatchCategoryCodes defines Manifest File BatchCategoryCodes that the State Hub return to the Requester. The following data elements define the attributes of the Manifest BatchCategoryCodes that the State Hub return to the Requester when an error has occurred.

*Table 18 - Response Manifest Schema: State Hub to Requester BatchCategoryCodes*



ASUME Response  
Manifest BatchCatego

#### 5.1.5.3.3 ASUME File Data Elements and ResponseCode

The following section details the request schema that shall be used to send the requests to the ASUME System and the response schema that shall be used to send the responses back to the Requestor System.

##### *5.1.5.3.3.1 ASUME Request Data Elements*

Figure 9 - High Level ASUME Request UML illustrates the elements that the ASUME request shall contain in order to submit the requests to the Local Interface. Detailed data elements are described in Table 19 - Request Data Elements: ASUME Batch Participant Information Interface to ASUME Batch System File Request

*Figure 9 - High Level ASUME Request UML*

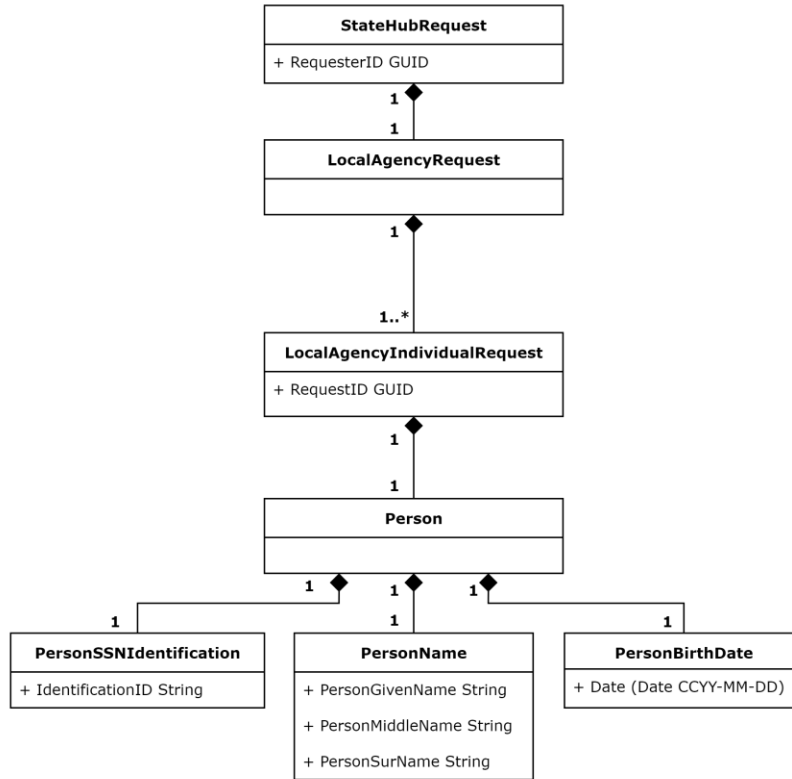


Table 19 - Request Data Elements: ASUME Batch Participant Information Interface to ASUME Batch System File Request defines the request data elements that the ASUME Batch Participant Information Interface needs to be submitted to the ASUME Batch System.



**ASUME Batch Participant Information: Interface Control Document (ICD)**

---

*Table 19 - Request Data Elements: ASUME Batch Participant Information Interface to ASUME Batch System File Request*



ASUME Request  
Data.xlsx

### *5.1.5.3.3.2 ASUME Response Data Elements*

Figure 10 - High Level ASUME Response UML illustrates the elements that the ASUME response shall contain in order to receive the responses from the Local Interface. Detailed data elements are detailed in Table 20.

*Figure 10 - High Level ASUME Response UML*



**ASUME Batch Participant Information: Interface Control Document (ICD)**

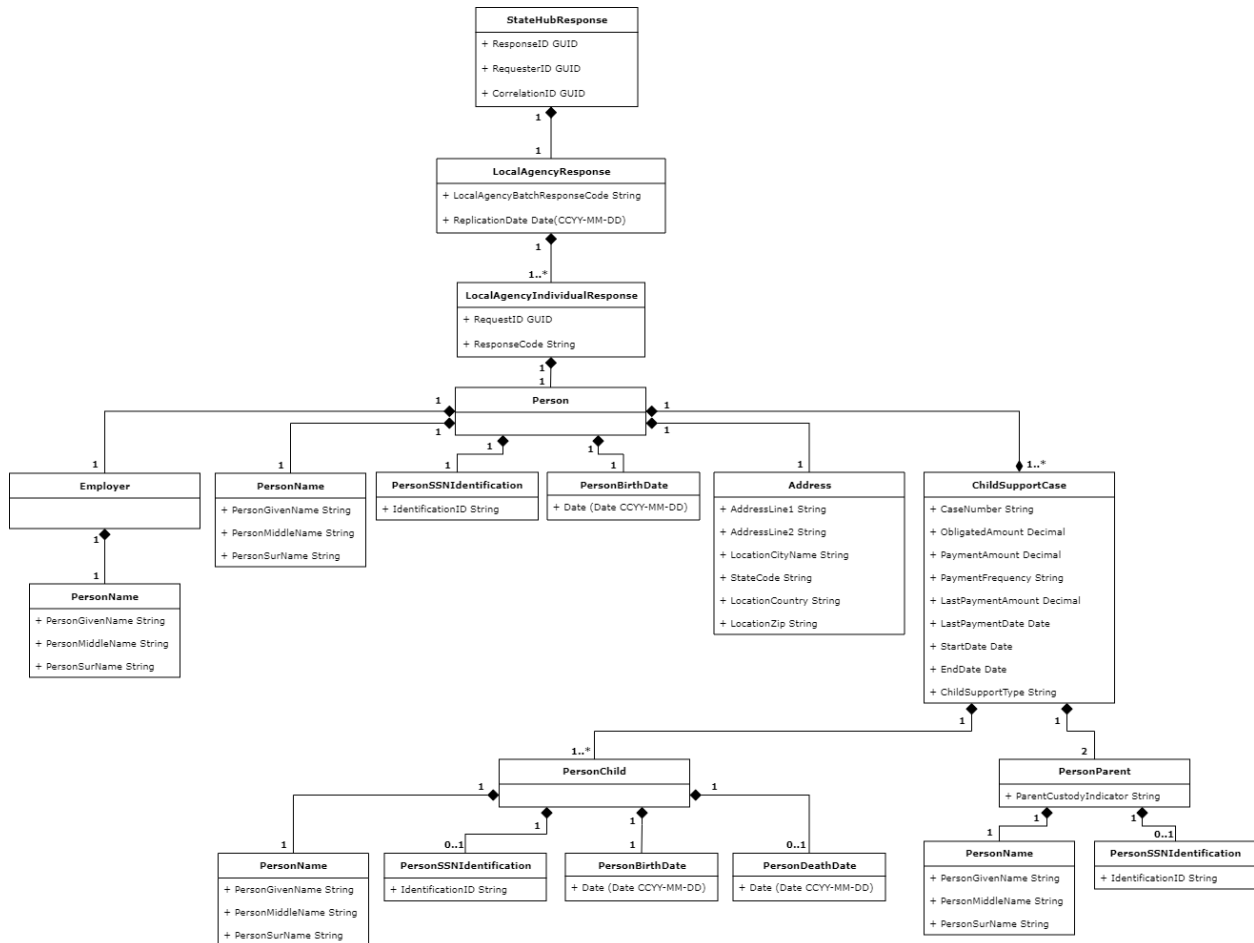


Table 20 - Response Data Elements: ASUME Batch System to ASUME Batch Participant Information Interface File Response defines the TDS response data elements that the ASUME Batch System needs to return to the ASUME Batch Participant Information Interface. The following data elements define the attributes of the TDS file that the ASUME Batch System need to return to the ASUME Batch Participant Information Interface.

*Table 20 - Response Data Elements: ASUME Batch System to ASUME Batch Participant Information Interface File Response*



ASUME Response  
Data.xlsx

5.1.5.3.3.3 ASUME ResponseCode

Table 21 - ResponseCode: ASUME Batch System LocalAgencyBatchResponseCode defines the TDS LocalAgencyResponseCode that the ASUME Batch System needs to return to the ASUME Batch Participant Information Interface for each segmented batch.

*Table 21 - ResponseCode: ASUME Batch System LocalAgencyBatchResponseCode*



ASUME Response  
Codes.xlsx

**Note:** The stored procedure is not expected to return SQL Exception error rather an XML with the error code 0099. Nonetheless, there shall be unexpected situations where the XML response to the SQL Exception shall not be possible and if that would be the case then the whole individual batch shall be considered to be under the 0099 error code.

Table 22 - ResponseCode: ASUME Batch System LocalAgencyIndividualResponse/ResponseCode defines the TDS LocalAgencyResponseCode that the ASUME Batch System needs to return to the ASUME Batch Participant Information Interface for each segmented batch.

*Table 22 - ResponseCode: ASUME Batch System LocalAgencyIndividualResponse/ResponseCode*



ASUME  
LocalAgencyIndividualR

### 5.1.6 Communication Methods

The following subsections outline the communication requirements for all aspects of the communication stack to which the systems participating in the interface shall conform.

Communication shall be divided three (3) ways:

- Bi-directionally between the Requestor System and the State Hub
- Within the Local Interface
- Bi-directionally between the Local Interface and TDS.



The Requestor System and the State Hub shall perform connections using an SSH-2 SFTP connection with RSA keys. These connections shall be done using a VPN tunnel which shall accept connections through the State Hub firewall. Inbound connections shall only be able to read and write in a very specific file directory, while outbound connections shall only read files from a different file directory. Packages sent through these connections are limited to request data files, response data files, and NACK XML files. See section 4.3 Data Transfer for detailed information on the folder structure and the composition of the ZIP file.

Within the Local Interface, the components shall communicate with each other using HTTPS requests and responses using REST and exchanging XML. The Local Interface shall also communicate with the SFTP to obtain and deposit request files and deposit response files using encryption in compliance with MARS-E.

The State Hub shall manage the request to the TDS using a VPN tunnel and transmitting data through TLS 1.2 to provide encryption. The packages being exchanged shall be XML for both the request and the response. The VPN tunnel shall enable the State Hub and the TDS access through ASUME's firewall to connect to the database and execute the Stored Procedure.

For exchange timing requirements see section 5.1.4: Interface Processing Time Requirements .

#### **5.1.6.1 Interface Initiation**

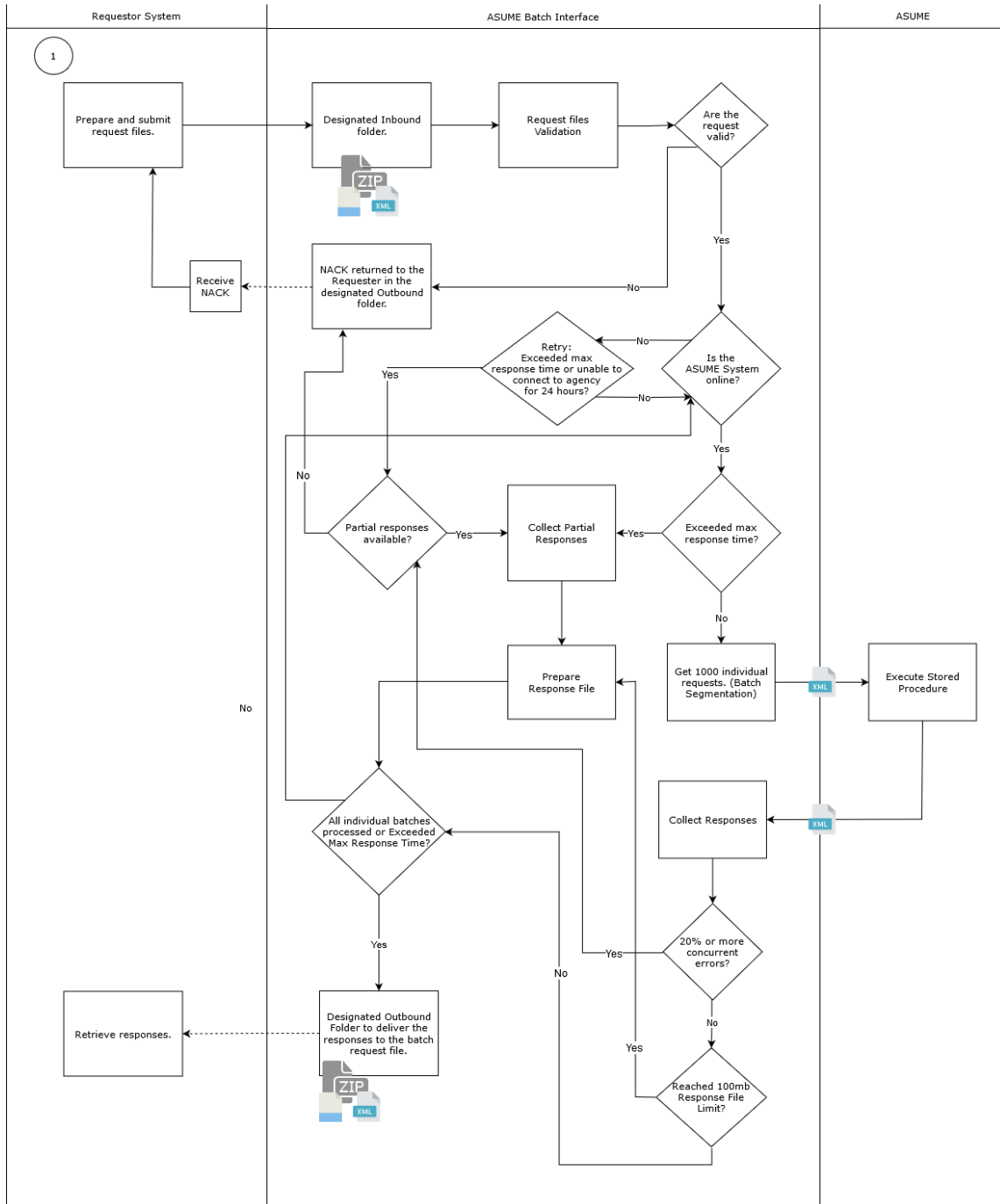
The Local Interface monitors the Inbound Folder by running a mechanism that shall be triggered when a new ZIP file has been deposited in the SFTP, the interface performs different validations to determine if the batch shall continue the workflow on the deposited files.

The connection to the SFTP server is through the SSH-2. The Requestor System shall provide the SFTP server the correct private key to be able to submit the file and initiate the interface execution.

### **5.1.6.2 Flow Control**

A high-level interaction between the Requestor System-Local Interface-ASUME can be seen in Figure 11 - ASUME Batch Participant Information Interface Process Flow.

*Figure 11 - ASUME Batch Participant Information Interface Process Flow*



The information regarding the NACK messages sent from the interface to the Requestor System can be found in sections 5.1.5.3.1.3: NACK Manifest ResponseCodes, 5.1.5.3.2.1: and 5.1.5.3.3.3: ASUME ResponseCode.



### 5.1.7 Security Requirements

All encryptions shall be done using 256-bit AES. This shall enforce HIPAA, HITECH 2009, FIPS 140-2 requirements as well as MARS-E requirements. Encryption shall be applied to requests, responses, and any data that is processed within the Local Interface and forwarded to ASUME or the Requestor System. Operations performed by the Local Interface shall go through a three (3) step process:

1. Decryption
2. Processing
3. Encryption

In other words: for every step of execution within the Local Interface, encryption shall always be managed with these three (3) steps to maintain encryption throughout all functionalities.

Data processed by the Local Interface shall also remain encrypted during interface functionality using HTTPS inside the virtual machines and cloud services layer of Azure Government's security model, which is its deepest layer. This data shall never be persisted in any way and shall only be accessible through memory so that it disappears from the State Hub and the Local Interface after any operation performed on it has been completed. Any reference to an operation in our reporting functionality and auditing functionality shall have no direct or indirect mention of the contents of the data that was processed when an alert or audit was performed. References to data values shall never be referenced in logging functionality which shall be limited to data fields or types only when it is necessary to reference them.

Connection to ASUME's database shall be handled and given by ASUME but shall be required to be encrypted using TLS 1.2 to access the Azure SQL 2016 database.

When connecting to the State Hub to perform requests with a request file, a VPN shall be required. Connection attempts that fall outside the bounds of the VPN shall not be accepted and the attempts shall be audited. Similarly, connection to ASUME's database shall be done using a separate VPN configured for connections between the State Hub and ASUME.

## 6 XML Schemas

This section provides schemas and examples for the schemas used to communicate the Requestor System with the ASUME System through the Local Interface.

### 6.1 Request and Response Manifest Schemas

Figure 12 - ASUME Request and Response Manifest Schema contains the ASUME Batch Participant Information manifest XML Schemas for submitting and receiving files. The samples in each ZIP file display examples of manifest schemas. Sections 5.1.5.3.1.1 – Request Manifest and 5.1.5.3.2.1 – Response Manifest provides detailed information on these schemas.

*Figure 12 - ASUME Request and Response Manifest Schema*



**Note:** The sample response manifest Schema is used for NACKS and Responses; therefore, the sample gives a depiction of all populated fields but not a true depiction of an actual scenario. See Section 4.3 Data Transfer for scenario depictions

### 6.2 ASUME Request and Response Schemas

Figure 13 - ASUME Request and Response File Schema contains the XML Schemas that the Requestor System shall use to communicate with the interface and the responses that shall be sent back. Additionally, this schema is used to communicate with the ASUME System Stored Procedure that the Local Interface interacts with. Section 5.1.5.3.3 provides detailed information on the ASUME request and response.

*Figure 13 - ASUME Request and Response File Schema*



**Note:** The sample used for the ASUME Request and Responses gives a depiction of all populated fields but not a true depiction of an actual scenario.



## 7 Qualification Methods

This ASUME Batch Participant Information ICD represents the delivery outcome of the evidence validation and interface analysis that has been gathered. Input from Puerto Rico Medicaid Program Subject Matter Experts and ASUME staff was collected during ASUME Batch JAD sessions and has been considered for this document as well. The qualification methods are aligned to the State Hub qualification methods, to see in detail refer to the Section 5 Release Management in the [State Hub HLD](#).

## 8 Related Documents

This section describes documents that support or are directly related to this document. See Table 23 - Related Documents.

*Table 23 - Related Documents*

Document	Reference
PREE Requirements and Definitions: Local Agency Interfaces Requirements (ASUME, ADSEF, Demographic Registry, DRNA)	<a href="https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/Deliverable%2015-%20Requirements%20and%20Definitions%20Document%20for%204%20Local%20Government%20Agencies%20Delivery?d=w01cde885bbb34d2ab08b7f310cc78dd1&amp;csf=1">https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/Deliverable%2015-%20Requirements%20and%20Definitions%20Document%20for%204%20Local%20Government%20Agencies%20Delivery?d=w01cde885bbb34d2ab08b7f310cc78dd1&amp;csf=1</a>
PREE Requirements and Definitions: State Data Verification Hub Requirements	<a href="https://intVOICEpr.sharepoint.com/EnE_P-APDU/_layouts/15/Doc.aspx?sourcedoc=%7BF165A982-4031-4AA4-996F-B2423C7BD5A3%7D&amp;file=PREE_StateHub_Requirements_and_Definitions_v1.0.docx&amp;action=default&amp;mobileRedirect=true&amp;DefaultItemOpen=1">https://intVOICEpr.sharepoint.com/EnE_P-APDU/_layouts/15/Doc.aspx?sourcedoc=%7BF165A982-4031-4AA4-996F-B2423C7BD5A3%7D&amp;file=PREE_StateHub_Requirements_and_Definitions_v1.0.docx&amp;action=default&amp;mobileRedirect=true&amp;DefaultItemOpen=1</a>
System Security Plan Document (SSP).	<a href="https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/PREE_Mediti3G_Audit/Working_folders/Wovenware_Documents?csf=1&amp;web=1&amp;e=jo5u5i">https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/PREE_Mediti3G_Audit/Working_folders/Wovenware_Documents?csf=1&amp;web=1&amp;e=jo5u5i</a>
PREE State Hub High Level Document	<a href="https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/WW_Deliverable%2004_HLD%20-%20State%20Data%20Verification%20Hub%20(NEW%20ARCHITECTURE)?d=wbe9e7869017d464aac340ebbd2bf35d7&amp;csf=1&amp;web=1">https://intVOICEpr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/WW_Deliverable%2004_HLD%20-%20State%20Data%20Verification%20Hub%20(NEW%20ARCHITECTURE)?d=wbe9e7869017d464aac340ebbd2bf35d7&amp;csf=1&amp;web=1</a>
ASUME Specification Document	<a href="https://intVOICEpr.sharepoint.com/EnE_P-APDU/Deliverables%20Library/WW-%20Deliverable%20139-ASUME%20Participant%20Information%20Local%20Agency%20Database%20Specification%20Document/Deliverable%20139-">https://intVOICEpr.sharepoint.com/EnE_P-APDU/Deliverables%20Library/WW-%20Deliverable%20139-ASUME%20Participant%20Information%20Local%20Agency%20Database%20Specification%20Document/Deliverable%20139-</a>

Document	Reference
	<a href="#">ASUME%20Participant%20Information%20Local%20Agency%20Database%20Specification%20Document.pdf</a>

## 9 Requirements Matrix

For requirement traceability purposes, the following requirements are met and mapped to this design document.

*Table 24 - General Functional Requirements*

Item #	ID	Requirement	Fit-Gap	Implementation Details
1	IR-GR-F-001	The real-time and batch local interfaces shall be hosted in the cloud as services.	Fit	
2	IR-GR-F-003	The batch local interfaces shall receive batch requests from the PREE System and route them to their corresponding local agency.	Fit	
3	IR-GR-F-005	The batch local interfaces shall deliver batch responses from their corresponding local agency to the PREE System.	Fit	
4	IR-GR-F-008	The batch local interfaces shall be able to accept one or more batch files for processing.	Fit	
5	IR-GR-F-009	The batch local interfaces shall send NACKS when a request was not processed due to a validation error, whether NIEM validation error, checksum validation error, or otherwise.	Fit	
6	IR-GR-F-010	The batch local interface shall return a response if the max agreed upon response time is exceeded. The response shall either be a NACK if whole response file has yet to be processed, or a response batch file with individual responses based on	Fit	



		batch processing completed against agency at that time.		
7	IR-GR-F-011	The real-time and batch local interfaces shall be uniquely identifiable from within the State Hub such that audit trails, log files, reporting services and other transactions can be quickly identified per local interface by the administrator user and auditor user when performing administrative tasks from the cloud portal.	Fit	
8	IR-GR-F-012	The real-time and batch local interfaces shall process all PII, PHI, and/or FTI in transit and shall not retain any PII nor PHI after the processing is completed.	Fit	
9	IR-GR-F-013	The batch local interfaces shall allow partial responses for batch transactions.	Fit	
10	IR-GR-F-015	The real-time and batch local interfaces shall support transporting inbound and outbound data to the PREE System adhering to the NIEM standard.	Fit	
11	IR-GR-F-016	The real-time and batch local interfaces shall send PII as search criteria to locate the person/participant at the local agency.	Fit	
12	IR-GR-F-017	The real-time and batch local interfaces shall be capable of receiving a response from their respective local agency with the participant information pre-defined data elements.	Fit	
13	IR-GR-F-018	The batch local interface shall allow PREE System to submit a batch request file for querying the local agency System for Participant(s) Information, to be returned within one or more response files.	Fit	
14	IR-GR-F-020	The batch local interface request file shall contain a batch set of individual participant requests, each request	Fit	



		containing participants PII search criteria.		
15	IR-AR-F-002	<p>The batch local interfaces shall log events resulting from requests received from the PREE System through the State Hub and the response from their corresponding local agency. At a minimum, events that shall be logged are:</p> <ol style="list-style-type: none"> <li>1. Batch file received for batch transactions.</li> <li>2. Size of the batch ZIP file in KB, MB, or GB</li> <li>3. Size of the batch file's XML document in KB, MB, or GB</li> <li>4. File validation results.             <ol style="list-style-type: none"> <li>a. Requester ID captured</li> </ol> </li> <li>5. Request transformation results (optional).</li> <li>6. Result of connectivity attempt to the local agency.             <ol style="list-style-type: none"> <li>a. Connection was established to the local agency (timestamp).</li> <li>b. Connection timeout between interface and local agency.</li> </ol> </li> <li>7. Agency query results             <ol style="list-style-type: none"> <li>a. Error code</li> </ol> </li> <li>8. Response transformation results (optional)</li> <li>9. Transaction completed after transmitting data to the local agency.</li> </ol> <p>Correlation ID captured.</p> <ol style="list-style-type: none"> <li>10. File placed for pick-up.</li> <li>11. File picked-up.</li> <li>12. File auto-removed.</li> </ol>	Fit	



16	IR-AR-F-003	The real-time and batch local interfaces shall log error codes accompanied by an unvarying, standard description that defines what the error code means when an exception occurs.	Gap	Further details will be provided in the Design Document.
17	IR-AR-F-004	The real-time and batch local interfaces shall relay audit trails related to warnings and errors to the State Hub using a normalized coding structure so that they are easily identifiable for auditing and troubleshooting purposes.	Gap	Further details will be provided in the Design Document.
18	IR-AR-F-005	The real-time and batch local interfaces shall not store PII, PHI, or FTI in audit trails.	Fit	
19	IR-AR-F-006	The real-time and batch local interfaces shall capture non-personal identifying invalid data in the communication (request and response) to help with troubleshooting.	Fit	
20	IR-SR-F-001	The real-time and batch local interfaces shall ensure that if a failure occurs, no sensitive information, such as PII, PHI, or FTI is vulnerable to external attacks via interface responses or captured audit trail.	Fit	
21	IR-SR-F-002	The real-time and batch local interfaces shall keep data encrypted during transit as originated from the PREE System and the Local Agency.	Fit	
22	IR-SR-F-003	The real-time and batch local interfaces shall establish a secure connection with the PREE System and the Local Agency.	Fit	
23	IR-SR-F-004	The batch local interfaces shall keep data encrypted at rest while the transaction is being processed.	Fit	
24	IR-SR-F-005	The batch local interfaces shall permanently remove all batch files, after the request has been processed and the response has been sent to the PREE System.	Fit	
25	IR-SR-F-006	The real-time and batch local interfaces shall comply with the	Fit	





		security guidelines and recommendations established in the Patient Protection and Affordable Care Act of 2010, Section 1561.		
26	IR-SR-F-007	The real-time and batch local interfaces shall comply with the security requirements established by the HITECH 2009.	Fit	
27	IR-SR-F-008	The real-time and batch local interfaces shall restrict access to appropriately authenticated systems (for example, PREE System and Local Agencies' Systems).	Fit	
28	IR-SR-F-009	The real-time and batch local interfaces shall restrict access to appropriately authenticated users (for example, administrator and auditor).	Fit	
29	IR-SR-F-010	The real-time and batch local interfaces shall allow an administrator, without granting read access, to delete an in-transit file (stuck in-transit).	Gap	Further details will be provided in the Design Document.
30	IR-SR-F-011	The batch local interfaces shall securely purge (delete) any file that reaches or surpasses the predefined time for processing.	Fit	
31	IR-GR-F-AS-002	The ASUME batch local interface shall validate batch files submitted by PREE System for message format compliance and integrity.	Fit	
32	IR-GR-F-AS-003	The ASUME real-time and batch local interfaces shall support the ability to retry a transaction, without manual intervention, after the local agency becomes unavailable mid-transaction.	Fit	
33	IR-GR-F-AS-004	The ASUME real-time and batch local interfaces shall be capable of returning, whenever available, a response with the replication date of the data.	Fit	
34	IR-GR-F-AS-005	The real-time and batch local interfaces shall capture metric of	Fit	

		whether the local agency endpoint is online or unavailable at the time of its use, up to including any retry attempts.		
35	IR-GR-F-AS-006	In case of connectivity issues between the batch local interface and the local agency, the local interface shall retry establishing connection and processing the transaction every half-hour (30 minutes) for up to the max response time or a consecutive 24-hour window of not communicating. Each attempt of reconnecting shall be notified to the State Hub.	Fit	

*Table 25 - Non-Functional Requirements*

Item #	ID	Requirement	Fit-Gap	Implementation Details
1	IR-GR-NF-004	The batch local interfaces shall process batch uncompressed XML files that do not exceed two hundred and fifty (250) Megabytes (MB).	Fit	
2	IR-GR-NF-005	The batch local interfaces shall be able to process up to one (1) request file at a time	Fit	
3	IR-GR-NF-006	The batch local interface shall expose an SFTP directory so that PREE System shall submit batch requests files for batch querying.	Fit	
4	IR-GR-NF-007	The batch local interface shall expose an SFTP directory so that PREE System shall pick up any batch response files destined for PREE System.	Fit	
5	IR-GR-NF-008	The batch local interfaces shall permanently remove in-transit files that has not been used within ten (10) calendar days.	Fit	
6	IR-GR-NF-009	The real-time and batch local interfaces shall comply with HIPAA	Fit	



Item #	ID	Requirement	Fit-Gap	Implementation Details
		and MARS-E regulations to guarantee data encryption, protection, portability, and integrity.		
7	IR-GR-NF-012	The batch interfaces shall support Application-to-Application asynchronous behavior for batch requests.	Fit	
8	IR-LR-NF-001	The real-time and batch local interfaces shall generate alerts and notifications through the State Hub using monitoring capabilities.	Gap	Further details will be provided in the Design Document.
9	IR-MR-NF-001	The real-time and batch local interfaces shall capture metrics on the availability of the service provider (local agency). The metric shall compliment the State Hub's service provide monitoring capabilities.	Gap	Further details will be provided in the Design Document.
10	IR-SR-NF-001	The real-time and batch local interfaces that support Secure Socket Layer (SSL) connections shall be supported by public key/private key encryption SSL certificates capable of 256-bit encryption or stronger.	Fit	
11	IR-SR-NF-002	The security configurations and conditions that the real-time and batch local interfaces are required to implement in a production environment shall be the same configurations and conditions implemented in all development, testing, integration, and acceptance test environments to guarantee compliance with the security measures in the MARS-E for protecting PII and PHI.	Fit	
12	IR-SR-NF-003	The real-time and batch local interfaces development and development tests shall not use real	Fit	



Item #	ID	Requirement	Fit-Gap	Implementation Details
		data for development or testing environments.		
13	IR-SR-NF-004	The batch local interfaces shall perform source to destination file integrity checks for exchange of data to ensure no corrupted data reaches to or is extracted from the local agency.	Fit	
14	IR-GR-NF-AS-001	The real-time and batch local interfaces shall be capable of receiving a response from ASUME with the following participant information data elements: <ul style="list-style-type: none"> <li>a. Absent Parent Child Support</li> <li>b. Absent Parent</li> <li>c. Address</li> <li>d. Birth and Death Details</li> <li>e. Child Support Expense</li> </ul>	Fit	
15	IR-GR-NF-AS-002	The ASUME batch local interfaces shall have a maximum response time of five (5) days.	Fit	
16	IR-GR-NF-AS-003	In case of connectivity issues between the batch local interface and the local agency, the local interface shall retry establishing connection and processing the transaction every half-hour (30 minutes) for up to the max response time or a consecutive 24-hour window of not communicating. Each attempt of reconnecting shall be notified to the State Hub.	Fit	
17	IR-SR-NF-AS-001	The ASUME real-time and batch local interfaces shall be hosted in a MARS-E secure environment.	Fit	



## 10 Issue Register

This section shall capture the identified issues that caused a change to the Local Interface.

*Table 26 - Issue Register*

Issue #	Issue	Resolution	Resolution Date
None identified at this moment			

## 11 Appendix A – ASUME API

ASUME provides a real time web service that provides information about an ASUME participant. The webservice also allows for the validation of certifications given by the Local Agency. Nonetheless, this API is not used since it does not provide all the information necessary to allow PRMP to determine eligibility for their beneficiaries. It was determined with ASUME to use an alternate means for this interface.

The documentation for the ASUME API is located at  
<https://serviciosonline.asume.pr.gov/asume.api/help>.