DEPARTAMENTO DE SALUD

# Deliverable 214- ICD: Puerto Rico Department of Treasury (Hacienda) Real Time Participant Information: Interface Control Document(ICD)

Mediti3G Project
Government of Puerto Rico

**Version 2.3**
**September 26, 2023**

**Contract # 2022- DS0707-E**

# Document Revision History

*Table 1 - Document Revision History*

| Version Number | Date | Description |
|---|---|---|
| **1.0** | 3/31/2021 | Submission of the document for approval. |
| **2.0** | 3/31/2022 | • Updated Document Revision History<br>• Updated Title Page, page i<br>• Updated Table 2 and Wovenware direction, page ii<br>• Updated section 1<br>• Updated section 1.1<br>• Update section 1.2<br>• Update section 1.3<br>• Update section 1.4<br>• Update section 2<br>• Update section 3<br>• Update section 3.2<br>• Update section 4<br>• Update section 5<br>• Update section 5.1.5.1<br>• Update section 5.1.5.3<br>• Update section 6.1<br>• Update section 7<br>• Update section 8<br>• Update section 13<br>• Update section 15 |
| **2.1** | 7/26/2022 | Made changes to reflect the new elements discussed with PRMP and Hacienda. |
| **2.2** | 10/24/2022 | Added tax return request constraint. No tax return prior 2020. Added Hacienda individual response codes. |
| **2.3** | 9/26/2023 | Updated Table 7: Income values may come from Schedule CO.<br>Updated Table 9: Individual Response Codes.<br>Updated Appendix B Hacienda Web Service Specification Document. |

# Document Approval

*Table 2 - Document Approval*

| Stakeholder Name | Stakeholder Role | Stakeholder Signature | Signature Date (MM/DD/YYYY) |
|---|---|---|---|
| **Alexander Quevedo** | State HIT Coordinator | | |

**Send inquiries to:**

**Wovenware**

**1000 Calle Los Angeles Suite 100**
**San Juan, PR 00909**
**E-Mail:**
**mediti3g@wovenware.com**

# Table of Contents

## LIST OF TABLES



## LIST OF FIGURES

# 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 MEDITI3G Initiative of the Puerto Rico Department of Health. The Department of Treasury (Hacienda, in Spanish "Departamento de Hacienda") Real-Time Participant Information Interface (henceforth Local Interface) is an interface between the MEDITI3G System and the Hacienda System.

The MEDITI3G System shall send a real time request to the interface to gather information about the applicant/beneficiary in the Hacienda System. The interface shall collect the information returned by Hacienda (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) records and tracks the information required to define the Local Interface. This establishes connection and interaction between the Requestor System and the Hacienda System. The connection bridges access to critical participant information from the Local Agency through the State Hub via real- time transactions.

The ICD establishes the specifications that the Local Interface shall contain in general:

- the connectivity standards between the systems
- the message formatting to communicate the systems
- the capabilities supported by the interface
- the security considerations required

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 is the income reported to the agency in the tax returns.

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

1. The MEDITI3G System shall submit the PRMP participant information requests to be processed by the Local Interface to look up the information in the Hacienda System by means of Real Time transactions.
2. The interface shall convert the responses to the standard format.
3. Simple data validations shall be done by the Local Interface. All specified/provided rules are explained in detail in section 5: Detailed Interface Requirements.
4. Log Local Interface audit trail.
5. Errors shall be classified as system or data errors and shall be logged independently within the Local Interface for reference purposes.
    1. System errors are those related (but not limited) to (1) an unexpected error while the interface processes the requested file.
    2. Data errors are those that occurred while enforcing the data validation rules described in section 5: Detailed Interface Requirements.
6. 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 guidelines rules, all extracted data shall be handled in the State Hub internal network and not be transmitted outside the network while being processed. The requests and responses shall not be persisted in the State Hub.

## 1.3 Team Members

*Table 3 - Team Members*

| Participants | Organization |
|---|---|
| Blake Hansard | PMO |
| Alexander Quevedo | PRMP |
| Irma Avilés | PRMP |
| Evelyn Santos | PRMP |
| Stephanie Nieves | RedMane |
| Brandon Peclyak | RedMane |
| Tamera Jones | Redmane |
| Victor Opio | Hacienda |
| Johana Rohena | Hacienda |
| Christy Schilling | Berry Dunn |

## 1.4 Glossary of Terms

*Table 4 - Glossary of Terms*

| Acronym/Term | Definition |
|---|---|
| **AES** | Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology. |
| **CMS** | Centers for Medicare & Medicaid Services |
| **DOB** | Date of Birth |
| **FIPS** | Federal Information Processing Standards |
| **Hacienda** | Puerto Rico Department of Treasury |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **HIT** | Health Information Technology |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **ICD** | Interface Control Document |
| **JSON** | JavaScript Object Notation |
| **MARS-E** | Minimum Acceptable Risk Standards for Exchanges |
| **MEDITI3G** | Medicaid Integrated Technology Initiative ("MEDITI") 3rd Generation |
| **NIEM** | National Information Exchange Model |
| **PII** | Personally Identifiable Information |
| **PMO** | Project Management Office |
| **PRDoH** | Puerto Rico Department of Health |
| **Requestor System** | Name to identify the solution used by the PRMP caseworkers for eligibility management. |
| **REST** | Representational state transfer architecture. |
| **PRMP** | Puerto Rico Medicaid Program |
| **SHA** | Secure Hash Algorithm |
| **SOAP** | Simple Object Access Protocol |
| **SSN** | Social Security Number |
| **TDS** | Trusted Data Source |
| **TLS** | Transport Layer Security |

| Acronym/Term | Definition |
|---|---|
| **UML** | Unified Modeling Language |
| **VPN** | Virtual Private Network |
| **WSS** | Web Services Security |
| **XML** | Extensible Markup Language |

# 2 Overview

The Puerto Rico Department of Treasury, henceforth Hacienda, is the executive department of the government of Puerto Rico responsible for the treasury of the U.S. Commonwealth of Puerto Rico. It is one of the constitutionally created executive departments. The Department collects taxes, operates the local lottery, and serves as the central disbursement agency of the government.

The Requestor System, through real time requests, shall query the Local Interface for information regarding an applicant's/beneficiary's information in a Local Agency. The real time requests shall contain an applicant/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 MARS-E, HIPAA Privacy Rule, HIPAA Security Rule, and CMS Standards and Conditions as the basis.

# 3 Assumptions/Constraints/Risks

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 Hacienda Real-Time Interface:

1. Azure Government shall maintain its current offerings of services and components. The inclusion of new offerings later will not negatively impact compatibility and compliance with HIPAA and MARS-E.
2. The Requestor System shall use the interface on a real-time basis to determine eligibility of PRMP beneficiaries.
3. The Requestor System shall request the Local Agency through the Local Interface only.
4. No transformation shall be performed on the request sent by the Requestor System. This applies to both, real-time and batch local interfaces.
5. Hacienda's real-time endpoint shall be available in a timely fashion unless otherwise notified to PRMP and Wovenware personnel. Core working hours are between 7:00 a.m. and 7:00 p.m. Atlantic Standard Time Monday through Friday.
6. The Hacienda environment configurations shall be compliant with applicable HIPAA and MARS-E regulations.
7. Hacienda shall communicate to PRMP security findings pertaining to the interfaces' end endpoints that might affect the normal operations as soon as they have been identified. For example, if there are server storage constraints, any maintenance outside of specified windows, any security incidents, etc.

## 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 a single Trusted Data Source (TDS) for requesting data.

2. 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.
3. Hacienda shall provide a citizen's non-Modified Adjusted Gross Income (non-MAGI) income information (lottery winnings, casino winnings, IVU winnings, and other winnings that are not considered an employment salary).
4. The Requestor System shall generate a real time interface SOAP request and send it through HTTPS to the Local Interface. The real time request contains an individual request with the applicant/beneficiary's personal identifiable information that can be used to locate the applicant/beneficiary's information within the agency's system, information such as SSN, Name, and Date of Birth (DoB).

## 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 Hacienda's System. In addition, it shall cover the security and integrity requirements needed for the request to be considered successful and achievable.

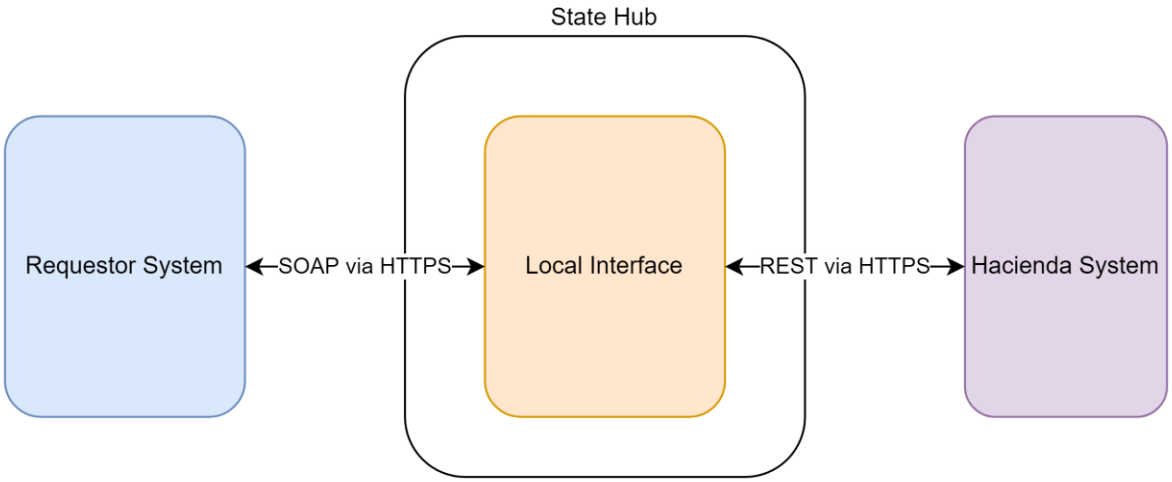
## 4.1 Interface Overview

The Local Interface residing in the State Hub shall connect the Requestor System with the Hacienda System seeking to acquire beneficiary's personal information.

1. The Requestor System shall generate a real time interface Simple Object Access Protocol (SOAP) request and send it through HyperText Transfer Protocol Secure (HTTPS) to the Local Interface. The real time request contains the participant personal identifiable information (individual request) to get in the agency's system such as SSN, Name, Date of Birth (DOB), and the requestor information. The real time request may contain up to 5 individual requests.
2. The interface shall validate the received request against the XML schema that is formatted in NIEM 2.0.
3. The interface shall create a JSON request to provide it to the Hacienda System via concurrent connections.
4. Upon locating a participant, the Local Agency shall respond with the participant's personal information, address, and income reported to the agency.
5. Once the real-time response has been received from the agency, the interface shall pass through the response to the Requestor System.
6. Alternatively, the interface may determine instead to return a response message with a response code back to Requestor System in the scenarios where the interface cannot process the submitted request, scenarios such as when the request fails validation. The response code shall inform of any error encountered during the process.
7. Finally, Requestor System shall receive the response from the Local Interface via HTTPS in a SOAP message.

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

*Figure 1 - Hacienda Real Time Participant Information Interface Enterprise Architecture*




In Figure 1, the Requestor System is the entity in charge of initiating the real time SOAP request via HTTPS with the Local Interface. The Hacienda System is the Local Agency system that the Local Interface shall interact with to query participants information. The Local Interface is hosted in the State Hub and shall connect with the Hacienda System REST endpoint via HTTPS and send a JSON message to perform the request sent by the Requestor System. The Local Interface shall send synchronously 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 initiates the service request to the Local Interface. As a result of this trigger, the Local Interface shall commence the business operation to process the individual request(s) against the Hacienda 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 is detailed in section 5.1.5 Message Format (or Record Layout) and Required Protocols.

The Local Interface shall be able to manage up to two thousand (2000) concurrent requests from the Requestor System and at least one thousand and five hundred (1,500) requests per hour.

If the Local Interface is unable to process the request on the first try, the interface shall retry up to three times (3) in twenty (20) seconds intervals, in a maximum response time of sixty (60) seconds. If the Local Interface reaches the sixty (60) seconds response time, the interface is to send the Requestor System a response message with the response code depicting the error.

## 4.3 Data Transfer

The State Hub and the Requestor System exchange real-time information through a service that supports synchronous calls between the two. Specifically, the exchange protocol used is via SOAP messages conforming to SOAP v1.2 using Hypertext Transfer Protocol Secure (HTTPS). Data follows a sequence of Request > Process > Respond with Results.

Figure 2 - SOAP Request Message to the State Hub for HTTPS Binding provides the basic SOAP request message structure for the service. The figure illustrates a request from the Requestor System to the Local Interface through the State Hub.

*Figure 2 - SOAP Request Message to the State Hub for HTTPS Binding*

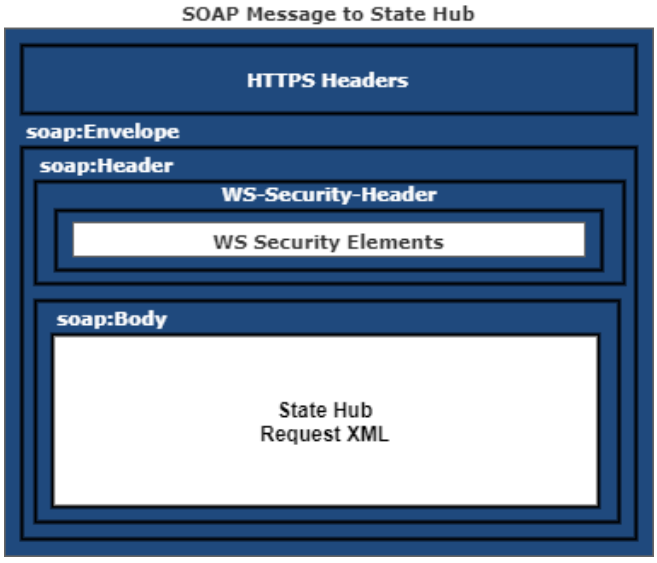



Figure 3 - SOAP Response Message to the MEDITI3G System for HTTPS Binding provides the basic SOAP response message structure for the service. The figure

illustrates a response from the Local Interface to the Requestor System through the State Hub.

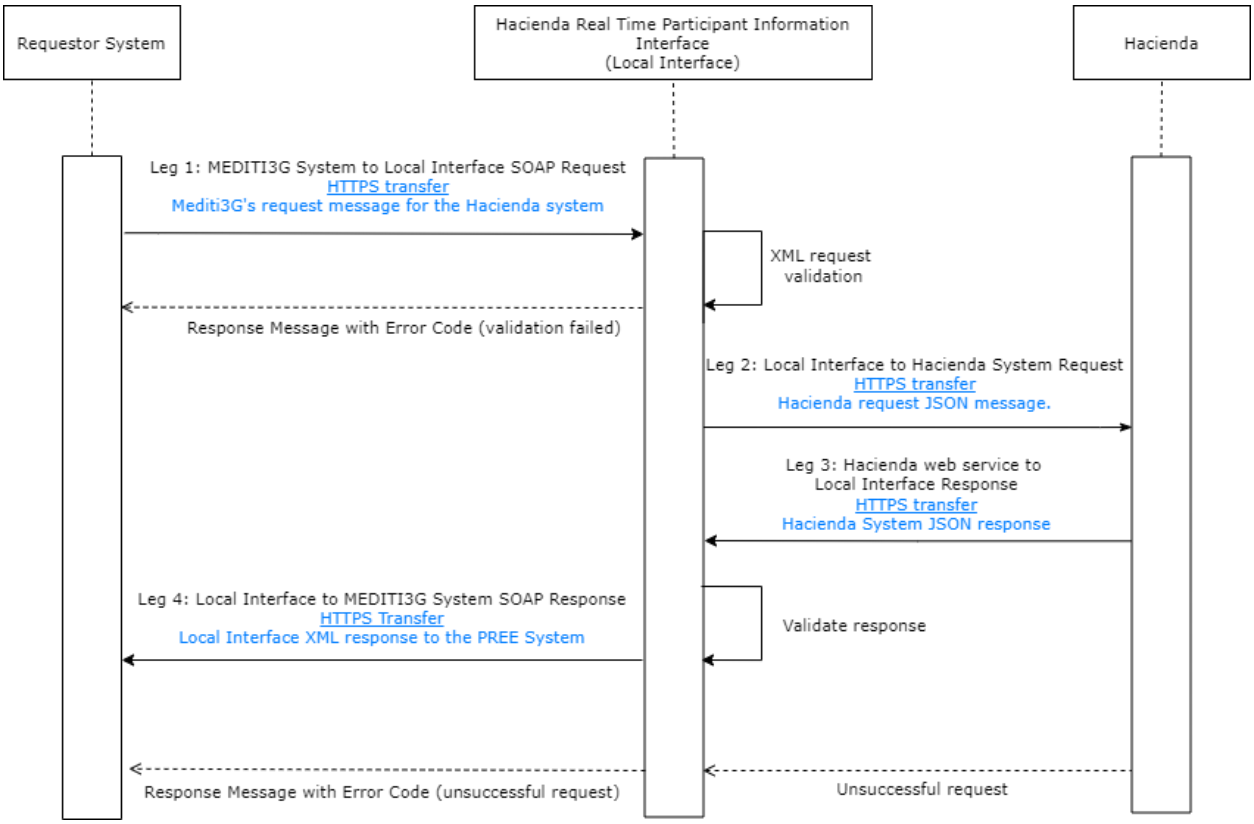
*Figure 3 - SOAP Response Message to the MEDITI3G System for HTTPS Binding*


When a validation error or a match error has occurred at the TDS, the interface shall receive a Response with Error from the TDS, containing information about the generated error and an error code to identify the type of error.

## 4.4 Transactions

The synchronous request transaction between Requestor System and Hacienda System is described below:

*Figure 4 - Transaction between MEDITI3G - Local Interface - Hacienda sequence*




Leg 1: Requestor System to Local Interface Request

- The Hacienda Real Time Participant Information Interface shall receive a real-time XML request following NIEM 2.0 standards. This transaction includes requests with personal identifiable information such as Full Name (First name and Last name), SSN, DOB, and requestor information.

Leg 2: Local Interface to Hacienda System Request.

- The interface shall process the requests against the Hacienda System via HTTPS. The query information shall be sent to the Hacienda System in XML

format. This transaction shall send the requests from Leg 1 to the Hacienda System via concurrent calls.

Leg 3: Hacienda System to Local Interface Response

- The interface shall receive the response from the Hacienda System and convert the result to XML format following NIEM 2.0 standards. This transaction includes the responses from the Hacienda System containing personal identifiable information, address, and the reported income to the agency.

Leg 4: Local Interface to Requestor System

- A SOAP response envelope is added to the response and delivered to the Requestor System via SOAP. This transaction shall take the responses from Leg 3 and deliver them to the Requestor System.

## 4.5 Security and Integrity

The Local Interface is to be hosted in the State Hub which provides a safe and secure environment. The State Hub allows for the Requesters to exchange data with the Local Agency in a safe and secure environment using services over HTTPS. This allows for secure and encrypted communication throughout the process. The connection between the Requestor System and the State Hub shall implement an X.509 certificate. An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to the user, computer, or service identity contained within the certificate. An X.509 certificate contains information about the identity to which a certificate is issued and the identity that issued it.

The Requestor System shall initiate the request following the message protocol SOAP. SOAP messages enable the State Hub and the Requester to send and receive data using services with data contracts. The protocol used to apply security to the SOAP messages is Web Services Security (WSS) and requires that each request sent contains a WSS header. The WSS header shall contain the UsernameToken that consist of information such as username and password. The identified MEDITI3G key personnel shall provide a username and password to the Requestor System to include it in its requests.

The State Hub contains auditing capabilities that provide information on the transactions from start to finish. The information captured includes information about the request; including the user that initiates the transaction, the origin, and the destination. The local interface shall audit message validations, connectivity attempts, transactions completed, and responses pulled. The interface shall be identifiable from within the audit logs of the State Hub.

The interface shall use Azure Government security rules to ensure that PII is not captured within the audit traces or payloads. These can be used as alerts or notifications and shall display information in a normalized coding structure.

The interface shall use Azure Government security rules to ensure that PII is not captured within the audit traces or payloads. The interface does employ the security mechanism to ensure that in case of a failure, no sensitive information such as PII is not visible or vulnerable to external attacks. Audit processes shall report any attempts to connect to the State Hub with relevant information.

All the technologies used to secure the entire process shall be HIPAA, HITECH 2009, FIPS 140-2, and Mars-E compliant, a detailed list shall be presented in section 5.1.7 Security Requirements .

# 5 Detailed Interface Requirements

The following section provides a detailed description of the interaction between the Requestor System and the Hacienda System through the interface in the State Hub.

## 5.1 Requirements for Hacienda Real Time Participant Information Interface

This Hacienda Real Time Participant Information interface shall be used to transfer requests from the Requestor System to Hacienda 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:

1. The participant's SSN has been pre-validated prior to a local interface match being requested for the Requestor System. Pre-validation shall be performed by PRMP manually or electronically.
2. Hacienda's network shall be configured to accept a maximum of one hundred (100) of concurrent connections.
3. The Local Agency shall promptly notify PRMP and Wovenware of any maintenance window not previously scheduled or agreed upon.
4. The TDS response shall include replicated timestamp.
5. Hacienda's endpoints shall provide the most up-to-date information available.
6. The Hacienda Real Time Environment shall have a scheduled downtime due to the replication process.
7. Real-time Local Interface shall handle a maximum of one hundred twenty thousand (120,000) transactions per month.
8. There shall be a peak usage of up to 30 case workers simultaneously using the Requestor System to query the real-time interface.
9. Hacienda's systems can support up to one hundred (100) simultaneous real-time transactions.
10. Hacienda's real-time endpoint shall be available in a timely fashion unless otherwise notified to PRMP and Wovenware personnel.

11. The Hacienda Real Time Interface shall interact with Hacienda through REST web service that resides on Hacienda's side, as agreed with the agency.
12. The TDS shall support up to 5 individual concurrent requests.
13. Hacienda shall provide an HTTPS REST endpoint to process the requests individually.
14. The Hacienda System shall support up to two thousand (2,000) parallel connections.
15. The Local Interface shall contain the data elements from the years 2020, 2021, and 2022.

### 5.1.2 Constraints

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

1. The Local Interface shall perform searches based on the combination:
   - SSN
   - First Name and Last Name
   - Date of Birth (DOB)

   Since all fields are needed, the ability to find a result with partially wrong information or miswritten values depends entirely on the matching algorithms of the Local Agency, if any.
2. 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.
3. The Hacienda System only supports individual requests.
4. The Hacienda System requires that the requester information is sent as part of the request to their system.
5. The Hacienda System does not provide tax return information prior 2020.

### 5.1.3 General Processing Steps

Table 5 - Hacienda Real Time Participant Information Interface Processing Steps details the processing steps that the interface completes on a case-by-case basis to process the requests from the Requestor System to the Hacienda System.

*Table 5 - Hacienda Real Time Participant Information Interface Processing Steps*

| Processing Step | Description | Responsible |
|---|---|---|
| **1** | The Requestor System is to provide a SOAP request to the Local Interface. | MEDITI3G |
| **2** | The Requestor System sends the synchronous request to the Hacienda System via the State Hub API Manager. | MEDITI3G |
| **3** | The Local Interface receives the request and validates it. | Local Interface |
| **4** | If the interface detects an error in validation, the interface shall send a response with an error code to the requestor system. | Local Interface |
| **5** | The Hacienda real-time request is a JSON format message. The interface shall convert from XML to JSON format request. | Local Interface |
| **6** | The Local Interface shall check if the Local Agency System is available. If the connection to the Local Agency is not established within three (3) retries in a sixty (60) second timeframe, the local interface shall stop the real-time transaction and a response message with an error code is returned. | Local Interface |
| **7** | The interface shall send the validated request to the Local Agency. | Local Interface |
| **8** | The interface shall receive the response from the Local Agency. | Local Interface |
| **9** | The responses received from the Local Agency are converted from JSON to XML and verified against the original request. If the Local Agency does not returned information or a response code for a participant, the Local Interface adds the participant to the response with the code 0050 (Unprocessed). If the information returned for any participant is invalid according to State Hub schemas, the PII of the participant is removed from the response and the code 9999 (Unsuccessful) is returned instead. | Local Interface |
| **10** | The response is returned to the Requestor System via SOAP. | Local Interface |

### 5.1.4 Interface Processing Time Requirements

The minimum response time of the Real Time request shall be within twenty (20) seconds, with a maximum response time of sixty (60) seconds.

In cases where the response time reaches the stated max response time of sixty (60) seconds, the response back to Requestor System shall be a response message with an error code. These shall be audited and presented in audit reports concerning exceeded the response time.

In the case where connections are not being established to the Hacienda System, the State Hub shall continue to retry the request every twenty (20) seconds, up to three (3) retries within the sixty (60) seconds.

### 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 Real Time requests to Hacienda and Hacienda shall respond to the requests sent by the Requestor System.

#### 5.1.5.1 File Layout

The Hacienda Real Time request and response messages are SOAP messages which payload is in XML format following NIEM standards for the Requestor System. Each SOAP request body sent by the Requestor System shall follow the format defined in section 5.1.5.3: Field/Element Definition.

#### 5.1.5.2 Data Assembly Characteristics

The data that is processed in the interface is in XML format following NIEM 2.0 standards. The real-time request can contain up to five (5) individual requests to the Hacienda System with information about the participant that is going to be matched. The request includes a request identifier, the name of the participant, the date of birth, and the social security number. On the other hand, the response created to the Requestor System includes up to five (5) individual responses, one for each requested participant, and the identifier for each request. Each participant's record returns the personal information stored, address(es), income reported and organization if apply.

The Hacienda Real Time Participant Information Interface file layouts are defined in section 5.1.5.3: Field/Element Definition.

### 5.1.5.3 Field/Element Definition

The following section details the request schema that shall be used to send the requests to the Hacienda System and the response schema that shall be used to send the responses back to the Requestor System. This section also provides details for errors 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.

### 5.1.5.4 Hacienda Real Time Request Data Elements

Figure 5 – High-Level Hacienda Request UML) diagram illustrates the elements that the Hacienda request shall contain in order to submit the requests to the Local Interface. Detailed data elements are described in Table 6 – Request Data Elements: Hacienda Real Time Participant Information Interface to Hacienda System File Request.

*Figure 5 – High-Level Hacienda Request UML*

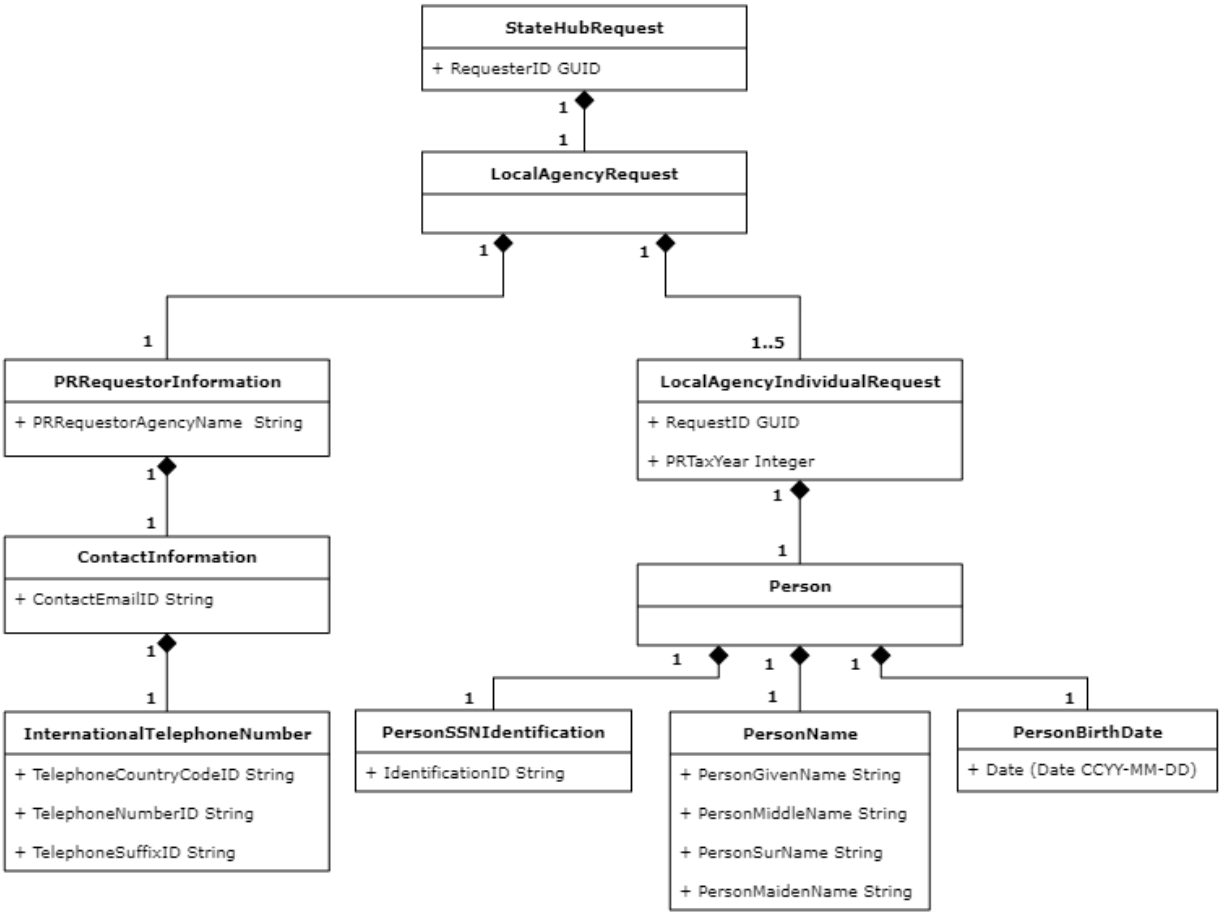



Table 6 – Request Data Elements: Hacienda Real Time Participant Information Interface to Hacienda System File Request defines the request data elements that the Hacienda Real Time Participant Information Interface needs to be submitted to the Hacienda System. The following data elements define the attributes of the TDS-destined file that the Hacienda Real Time Participant Information Interface need to submit to the Hacienda System.

*Table 6 – Request Data Elements: Hacienda Real Time Participant Information Interface to Hacienda System File Request*

HaciendaRequestDataElements.xlsx

### 5.1.5.5 Hacienda Real Time Response Data Elements

Figure 6 - High Level Hacienda Response UML illustrates the elements that the Hacienda response shall contain in order to receive the responses from the Local Interface. Detailed data elements are described in Table 7 – Response Data Elements: Hacienda System to Hacienda Real Time Interface File Response .

*Figure 6 - High Level Hacienda Response UML*

Hacienda RT HL Response UML.pdf

Table 7 defines the TDS response data elements that the Hacienda System needs to return to the Hacienda Real Time Participant Information Interface and returned to the Requestor System. The following data elements define the attributes of the response that the Local Interface needs to return to the Requestor System.

*Table 7 – Response Data Elements: Hacienda System to Hacienda Real Time Interface File Response*

HaciendaRTResponseDataElements.xlsx

### 5.1.5.6 Hacienda ResponseCode

Table 8 - ResponseCode: Hacienda System ResponseCode to Hacienda Real Time Interface and Requestor System defines the TDS responseCode that the Hacienda System needs to return to the Hacienda Real Time Participant Information Interface and the Requestor System.

*Table 8 - ResponseCode: Hacienda System ResponseCode to Hacienda Real Time Interface and Requestor System*

Hacienda Response Codes.xlsx

Table 9 - ResponseCode: Hacienda System LocalAgencyIndividualResponse/ResponseCode defines the TDS LocalAgencyResponseCode that the Hacienda System needs to return to the Hacienda Real Time Participant Information Interface and Requestor System within the response.

*Table 9 - ResponseCode: Hacienda System LocalAgencyIndividualResponse/ResponseCode*

HaciendaIndividual ResponseCodes.xlsx

### 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 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 exchange data using SOAP version 1.1 requests via an HTTPS connection. Packages sent through these connections are limited to SOAP request data, SOAP response data, and SOAP response with error. See section 4.3 Data Transfer.

Within the Local Interface, the components shall communicate with each other using HTTPS requests and responses using Representational State Transfer (REST, an architectural style for developing web services) and exchanging XML. The security within the communication within these components is Transport Layer Security (TLS 1.2), cryptographic protocols designed to provide communications security over a computer network.

The Local Interface and the Local Agency shall exchange data using a JSON request via REST protocol in HTTPS. The REST web service that the Local Agency provides uses token authentication for the requests that the Local Interface shall send to the Local Agency.

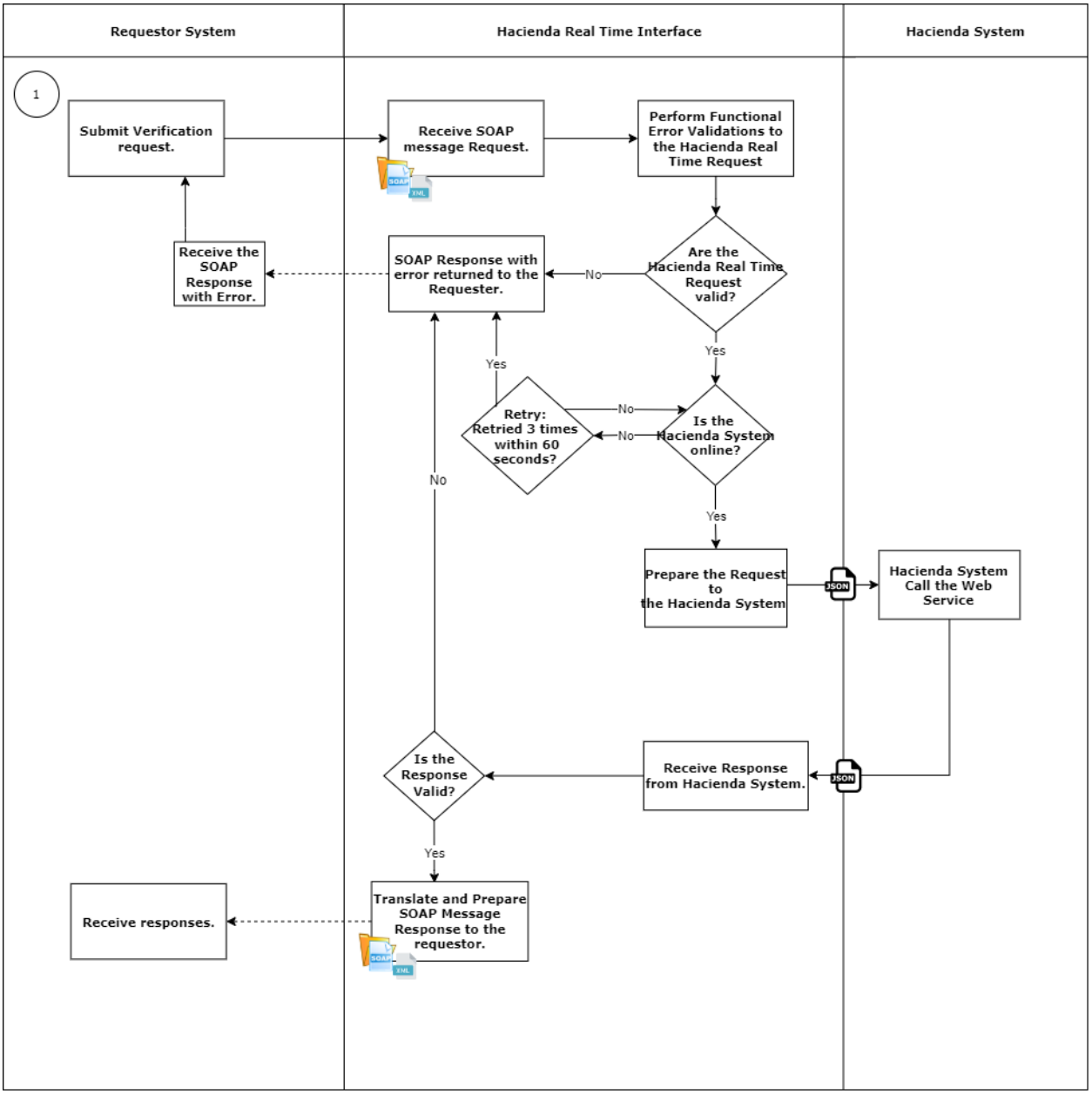
#### 5.1.6.1 Interface Initiation

The Local Interface initiates when the Requestor System sends the SOAP request to the Local Interface. Once the Local Interface receives the request, the interface performs different validations to determine if the request shall be queried against the Hacienda System.

#### 5.1.6.1 Flow Control

A high-level interaction between the Requestor System-Local Interface-Hacienda can be seen in Figure 7 - Hacienda Real Time Participant Information Interface Process Flow.

*Figure 7 - Hacienda Real Time Participant Information Interface Process Flow*




The information regarding the responses with error sent from the interface to the Requestor System can be found in sections 5.1.5.3.2 Hacienda Response Data Elements and 5.1.5.3.3 Hacienda ResponseCode.

### 5.1.7 Security Requirements

All encryptions shall be done using 256-bit Advanced Encryption Standard (AES). This shall enforce HIPAA, HITECH 2009, FIPS 140-2, and MARS-E requirements. Encryptions shall be applied to requests, responses, and any data that is processed within the Local Interface and forwarded to Hacienda 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.

Transport encryption shall be provided by TLS 1.2. This ensures that any request and response being transported between the Requestor System and the State Hub, as well as any request and response, have been done via requests to Hacienda's data store are secure while in transit. TLS 1.2 also enforces FIPS 140-2 requirements, which shall be primarily used in connections from the Requestor System to the State Hub, and from the State Hub to Hacienda's System.

Data processed by the Local Interface shall also remain encrypted and swapped during interface functionality using HTTPS inside the 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.

Access to the Azure Government environment, where the State Hub and the Local Interface reside, shall be limited to authorized personnel limited to the environment itself. These accounts shall be limited only to the maintenance of the interface. In other words, authorized accounts for Azure Government shall not have access to the State Hub API Manager and its idle requests and response messages.

# 6 XML Schemas

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

## 6.1 Local Interface WSDL (SOAP schemas)

*Figure 8 - Hacienda Real Time Interface WSDL*

HaciendaRealTime.xml

## 6.2 Hacienda Request and Response Schemas (NIEM schemas)

Figure 9 - Hacienda Request and Response Schema contains the XML Schemas that the Requestor System populates for the Hacienda destined requests and XML Schema that return to the Requestor System from Hacienda via the State Hub. Section 5.1.5 provides detailed information on the Hacienda request and response.

*Figure 9 - Hacienda Request and Response Schema*

Hacienda RT Request Response S

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

# 7 Qualification Methods

This Hacienda Real Time 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 Hacienda staff was collected during Hacienda Real Time 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 10 - Related Documents.

*Table 10 - Related Documents*

| Document | Reference |
|---|---|
| (HACIENDA)_Requirements and Definitions Document for Local Government Agency | https://intervoicepr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/Deliverable%20%2317%20-%20(HACIENDA)_Requirements%20and%20Definitions%20Document%20for%20Local%20Government%20Agency%20%235?d=w7a6c3a1b2c794ad6bd224b10a012a6e9&csf=1&web=1 |
| PREE Requirements and Definitions: State Data Verification Hub Requirements | https://intervoicepr.sharepoint.com/EnE_P-APDU/_layouts/15/Doc.aspx?sourcedoc=%7BF165A982-4031-4AA4-996F-B2423C7BD5A3%7D&file=PREE_StateHub_Requirements_and_Definitions_v1.0.docx&action=default&mobileredirect=true&DefaultItemOpen=1 |
| System Security Plan Document (SSP). | https://intervoicepr.sharepoint.com/:f:/r/EnE_P-APDU/PREE Mediti3G Audit/Working folders/Wovenware Documents?csf=1&web=1&e=jo5u5i |
| PREE State Hub High Level Document | https://intervoicepr.sharepoint.com/:f:/r/EnE_P-APDU/Deliverables%20Library/WW_Deliverable%20204_HLD%20-%20State%20Data%20Verification%20Hub%20(NEW%20ARCHITECTURE)?d=wbe9e7869017d464aac340ebbd2bf35d7&csf=1&web=1 |

# 9 Requirements Matrix

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

*Table 11 - 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-002 | The real-time local interfaces shall receive real-time requests from the Mediti3G System and route them to their corresponding local agency. | Fit | |
| 3 | IR-GR-F-004 | The real-time local interfaces shall deliver real-time responses from their corresponding local agency to the Mediti3G System. | Fit | |
| 4 | IR-GR-F-006 | The real-time interfaces shall implement Application to Application synchronous messaging behavior for real-time requests. | Fit | |
| 5 | IR-GR-F-007 | The real-time local interfaces shall respond real-time transactions back to the Mediti3G system within a pre-agreed response time. | Fit | |
| 6 | 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 | |
| 7 | IR-GR-F-012 | The real-time and batch local interfaces shall process all PII in transit and shall not retain any PII after the processing is completed. | Fit | |

| | | | | |
|---|---|---|---|---|
| 8 | IR-GR-F-014 | The real-time local interfaces shall allow sending and receiving multiple transactions in parallel within a specified limit of attempts. | Fit | |
| 9 | IR-GR-F-015 | The real-time and batch local interfaces shall support transporting inbound and outbound data to the Mediti3G system adhering to the NIEM standard. | Fit | |
| 10 | 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 | |
| 11 | IR-GR-F-017 | The real-time and batch local interfaces shall receive a response from their respective local agency with the participant information pre-defined data elements. | Fit | |
| 12 | IR-GR-F-019 | The real-time local interface shall allow Mediti3G System to submit a real-time request for querying the local agency System for Participant(s) Information, to be returned within one response. | Fit | |
| 13 | IR-AR-F-001 | The real-time local interfaces shall log events resulting from requests received from the Mediti3G System and the response from their corresponding local agency. At a minimum, events that shall be logged are:<br><br>1. Request is received.<br>a. Requester ID captured<br>2. Message validation.<br>3. Transformation (optional).<br>4. Result of connectivity attempt to the local agency.<br>a. Connection was established to the local agency (timestamp).<br>b. Connection timeout between interface and local agency.<br>5. Retry history in case of a timeout occurring.<br>6. Response is issued.<br><br>Source ID captured | Fit | |
| 14 | IR-AR-F-003 | The real-time and batch local interfaces shall log error codes accompanied by an | Fit | |

| | | | | |
|---|---|---|---|---|
| | | unvarying, standard description that defines what the error code means when an exception occurs. | | |
| 15 | 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. | Fit | |
| 16 | IR-AR-F-005 | The real-time and batch local interfaces shall not store PII in audit trails. | Fit | |
| 17 | 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 | |
| 18 | IR-SR-F-001 | The real-time and batch local interfaces shall ensure that if a failure occurs, no sensitive information, such as PII, is vulnerable to external attacks via interface responses or captured audit trail. | Fit | |
| 19 | IR-SR-F-002 | The real-time and batch local interfaces shall keep data encrypted during transit as originated from the Mediti3G System and the Local Agency. | Fit | |
| 20 | IR-SR-F-003 | The real-time and batch local interfaces shall establish a secure connection with the Mediti3G System and the Local Agency. | Fit | |
| 21 | IR-SR-F-006 | The real-time and batch local interfaces shall comply with the security guidelines and recommendations established in the Patient Protection and Affordable Care Act of 2010, Section 1561. | Fit | |
| 22 | IR-SR-F-007 | The real-time and batch local interfaces shall comply with the security requirements established by the HITECH 2009. | Fit | |
| 23 | IR-SR-F-008 | The real-time and batch local interfaces shall restrict access to appropriately authenticated systems (for example, Mediti3G System and Local Agencies' Systems). | Fit | |
| 24 | IR-SR-F-009 | The real-time and batch local interfaces shall restrict access to appropriately | Fit | |

| | | | | |
|---|---|---|---|---|
| | | authenticated users (for example, administrator and auditor). | | |
| 25 | 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). | Fit | |
| 26 | IR-GR-F-AD-001 | Hacienda real-time and batch local interfaces shall provide the data elements in section 11.1 upon request, whether by real-time or batch. | Fit | |
| 27 | IR-GR-F-HA-001 | The Hacienda 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 | |
| 28 | IR-GR-F-HA-002 | The Hacienda real-time and batch local interfaces shall capture metrics of whether the local agency endpoint is online or unavailable at the time of its use, up to including any retry attempts. | Fit | |
| 29 | IR-GR-F-HA-003 | The Hacienda real-time local interface shall validate request files submitted by Mediti 3G System for message format compliance and integrity. | Fit | |

*Table 12 - Non-Functional Requirements*

| Item # | ID | Requirement | Fit-Gap | Implementation Details |
|---|---|---|---|---|
| 1 | IR-GR-NF-001 | The real-time local interfaces shall support the implementation of HTTPS for message transportation between the Mediti3G System and the local interfaces. | Fit | |
| 2 | IR-GR-NF-002 | The real-time local interfaces shall be able to process at least one thousand five hundred (1,500) transactions per hour, including a peak of 30 concurrent calls. | Fit | |
| 3 | IR-GR-NF-003 | The real-time local interfaces shall be able to process up to five (5) individual requests within a single real-time request. | Fit | |

| | | | | |
|---|---|---|---|---|
| 4 | IR-GR-NF-009 | The real-time and batch local interfaces shall comply with HIPAA and Mars-E regulations to guarantee data encryption, protection, portability, and integrity. | Fit | |
| 5 | IR-GR-NF-010 | The real-time local interfaces shall have a response time of 20 seconds. | Fit | |
| 6 | IR-GR-NF-011 | In case of a connectivity issue between the real-time local interface and the local agency, the local interface shall retry the transaction for a maximum of 3 times, 20 second-limit per retry, before returning a response message to the Mediti3G system with the appropriate error code. Each attempt of reconnecting shall be notified to the State Hub. | Fit | |
| 7 | 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. |
| 8 | 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. |
| 9 | 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 with 256-bit encryption or stronger. | Fit | |
| 10 | 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. | Fit | |

| | | | | |
|---|---|---|---|---|
| 11 | IR-SR-NF-003 | The real-time and batch local interfaces development and development tests shall not use real data for development or testing environments. | Fit | |
| 12 | IR-GR-NF-HA-002 | The real-time and batch local interfaces shall receive a response from HACIENDA with the following participant information data elements:<br><br>a. Income snapshot<br>b. Resources (Non-MAGI)<br>c. Address<br><br>Identification Details | Fit | |
| 13 | IR-SR-NF-AS-001 | The HACIENDA 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 13 - Issue Register*

| Issue # | Issue | Resolution | Resolution Date |
|---|---|---|---|
| None identified at this moment | | | |

# 11 Appendix A – Hacienda Connectivity and Maintenance Plan

The following section provides a summary of the plan that Wovenware has been able to arrange with Hacienda for this Local Interface:

1. The Local Agency shall promptly notify PRMP and Wovenware of any maintenance window not previously scheduled or agreed upon.
2. The Hacienda Real-Time Participant Information Interface shall interact with Hacienda through the real-time request endpoint that resides in the State Hub, as agreed with the agency.
3. If the request is invalid or empty, the Local Agency shall return a response with an error to the Hacienda Real-Time Interface.
4. Hacienda shall provide access to the system that the Hacienda real-time participant information interface shall interact in their production environment that shall be hosted on-premises in their headquarters.
5. The Hacienda Real-Time Interface shall interact with Hacienda through a secure REST web service implemented on Hacienda's side, as agreed with the agency.
6. Hacienda's network may need to be configured to accept many concurrent connections.
7. The Hacienda System shall support up to 5 individual requests on a single call for real time processing.
8. Hacienda's REST web service shall be implemented to let the Local Interface only extract data and shall not make changes to Hacienda's data.

# 12 Appendix B – Hacienda REST Web Service Specification Document

Figure 10 - contains the suggested request and response JSON layout to exchange data between the Local Interface and the Hacienda System, and the authentication details with the system.

*Figure 10 - Hacienda REST Web Service Specification Document*


MEDITI3G - REST
Service Specifications