Use Cases

v1.1

IDB OPS Organización Panamericana de la Salud Organización Mundial de la Salud Américas RACSEL RED AMERICANA DE COOPERACIÓN SOBRE SALUD ELECTRÓNICA CENS CENTRO NACIONAL EN SISTEMAS DE INFORMACIÓN EN SALUD

Index

LACPASS - USE CASES

Regional Public Good (BPR) "Digital Transformation in Health to Mitigate the Effects of COVID-19 in Latin America and the Caribbean" (RG-T3769)

1. General Objective:

This document describes the use cases that will be considered during the second component of the LACPASS project and on which proof of concept tests will be performed. The use cases will cover as required: International Patient Summary (IPS) and Certificate of Vaccination (DDCC). Additionally an optional one related to signature mechanisms based on decentralized verification (LACCHAIN).

The three use cases or tracks considered for the second LACPASS Conectaton are summarized in Figure 01 below:

1.1 Specific technical objectives:

1. Implement the services defined for each country node, available in the Docker LACPASS.
2. Generate valid IPS as defined in the profile, using Docker LACPASS tools.
3. Log in to the LACPass-LACChain Regional Trust Registry
4. Exchange and validate IPS issued within the same country and by other participating countries.
5. Generate vaccination certificate from subset of IPS immunization data using Docker LACPASS tools.
6. Exchange and validate vaccination certificates issued within the same country and by other participating countries.

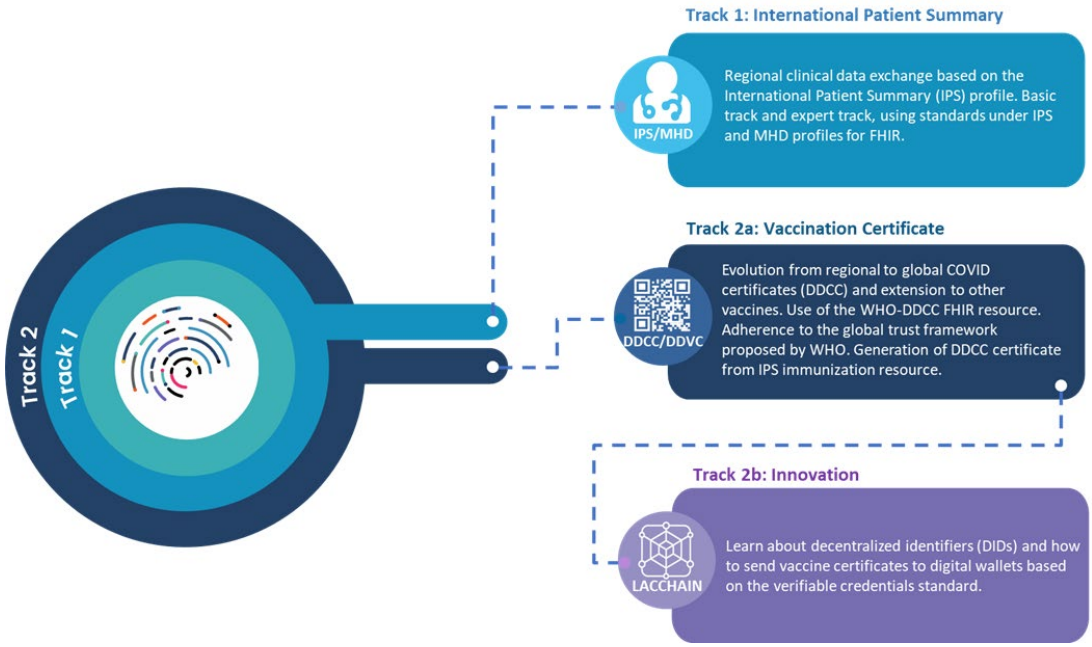


Fig.01: Summary of LACPASS proposal for tracks Conectaton

1.2 LACPASS Conectaton Tracks: The 2nd version of the LACPASS Conectaton considers 2 tracks (summarized in Figure 01) based on the enablers that are considered essential for the LAC region.

Track 1 International Patient Summary: The objective of this track is for each of the participants to succeed in generating their own valid international patient summary based on the IPS profile and interoperate with other countries according to MHD transactions. It considers the specific objectives 1.1.1 to 1.1.4: FHIR standard, IPS profile, MHD profile. LACPASS Docker.

Track 2a Vaccination Certificate: The objective of this track is for each of the participants to succeed in generating and interoperating a vaccination certificate, based on the DDCC/DDVC profile. It considers the objectives 1.1.3, 1.1.5 and 1.1.6: FHIR standard, WHO DDCC, LACPASS Docker.

Track 2b Innovation: It is proposed as an optional complement to the second track. The objective of this track consists of onboarding the health authorities of a country and their credentials in the LACPass trusted registry, as well as cryptographically verifying the keys of the authorities that sign the international patient summaries and DDCC vaccination certificates. Learn about digital identification and authentication (DIDs), digital wallets, and issuance/verification of vaccination certificates on the LACChain blockchain network. Consider objectives 1.1.3; 1.1.4 and 1.1.6. Basic knowledge of blockchain, X.509 Standard, LACCHAIN onboarding.

1.3 Preconectaton Phase

Contemplates the previous activities required for the execution of the proofs of concept under the framework of the 2nd LACPASS Connectathon.

- Registration: The registration stage for the 2nd LACPASS Conectaton is executed 3 months prior to the event and considers the creation of users in the Gazelle testing platform, the registration of the systems of the participating entities, and the selection of the tracks in which the entities will participate.
- Connectivity: This activity consists of the steps required for the systems of the participating countries to be able to interoperate with the Gazelle test platform.
- Pre-test: This activity is performed prior to the Conectaton and presents the tests parameterized in the Gazelle platform and the test flows.

2. Use Cases:

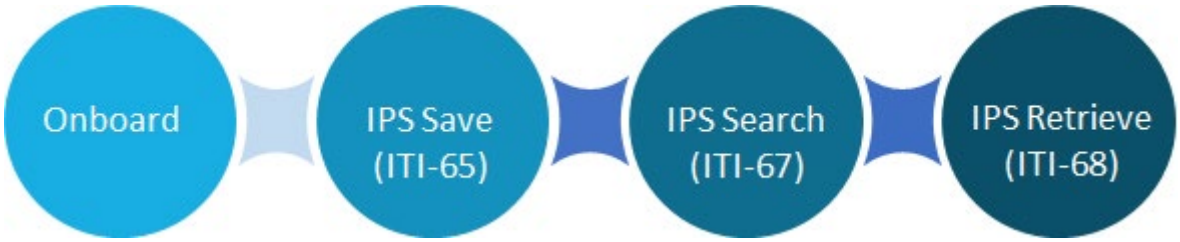
Based on the above definitions, the execution of a second LACPASS Conectaton is proposed to cover the following test cases:

1. (M) Initialize the CountryNode;
2. (M) Persist and validate test patient IPS: International patient summary;
3. (M) Enter the LACPass/LACChain Regional Trust Registry;.
4. (O) Revoke keys to the Regional Trust Register;
5. (M) Persist DDCC: Certificate of vaccination for COVID;
6. (O) Persist DDCC: Certificate of vaccination for different pathogens (e.g. yellow fever);
7. (O) Issuance of international certificates from DDCC-COVID. Ex: EU-DCC, SHC, etc;
8. (M) Verify/Validate own vaccination certificate;
9. (O) Verify/Validate vaccination certificate from other countries

3. Verification milestones:

The following are the milestones that will be verifiable during the connectathon exercise for each participating country.
They will be detailed under the following progress structure, in order to achieve a quantitative weighting of the achievements obtained during the exercise.

Regional data exchange



Digital certificates

4. Connectathon test architecture

The scenario to be configured for testing during the "connectathon" activity is detailed below:

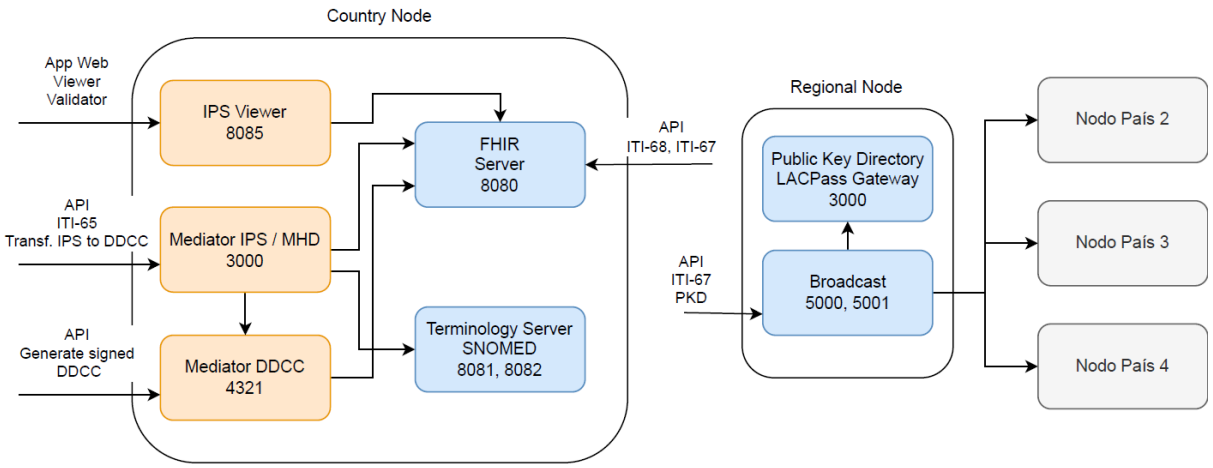


Fig.02: LACPASS proposal for proof of concept.

The diagram in Figure 2 shows the project architecture, which is divided into 2 actors: the Regional Node and the Country Node. The Regional Node is a series of services used for the orchestration and coordination of the country nodes, this node is developed and implemented by the LACPass technical team for testing during the connectathon. The Country Nodes correspond to services that each country must build locally in its infrastructure and include all the services necessary to execute the conectathon use cases. In the design of the architecture, a system was chosen in which the regional node has the least amount of services possible and most of the services are decentralized in the nodes of each country.

Each of the actors and modules involved are detailed below.

Regional Node.

- **Public key repository:** This is a repository where participating countries will upload their public keys used to sign system transactions and also the certificates obtained. It is public so that any country can obtain this information at any time to verify the authenticity of the documents.

- **Broadcast:** Corresponds to a service that allows a transaction query to be forwarded and issued to all the country nodes of the participating countries (broadcast). In this way, all Country Nodes can be consulted from a centralized point. This service also offers an API to register a Country Node and obtain a list of all registered Country Nodes, so that countries can decide to implement queries directly if they prefer.

Country Node.

- **National Backend:** Corresponds to a service that countries must implement to comply with the clinical information exchange service. The national backend must respond to at least 3 actions:

  - Indicate whether a patient with a certain ID is in the country's patient registry.

  - Generate the IPS file for a specific patient including as much information as possible.

  - Sign the contents of the IPS using a private key associated with the public key shared in the public key repository.

- **Terminology server:** Corresponds to a SNOWSTORM terminology server with the standard terms to be used in the IPS resource, among them are the SNOMED codes of the IPS free-set, ICD-10 or ICD-11 codes, specific valuesets for certain standards such as EU-DCC, and any other set of standard values required for the implementation. Ideally the terms will be available in English and Spanish.

- **IPS Node:** A service will be developed to validate the correctness of an IPS resource. The validation occurs in several stages, e.g., that it is syntactically correct, that it contains the required header information and values, that the values used are in the standard value set of the terminology server and that all information is available within the IPS resource including references.

- **FHIR Server:** A HAPI FHIR server instance will be set up for countries to add and query other resources. The FHIR server will host the information needed to build the IPS and will also respond to transactions that are sent.
- **Auxiliary Microservices An** API will be developed in the form of microservices with basic and specific functionalities that most countries will require in their national backend implementations. This API will be free to use by the countries and they can choose whether or not to use it in their implementation. Among the functionalities of this API will be: upload public keys to the PKD, verify the signature of an IPS certificate with the PKD keys, query concepts to the terminology server, convert from simple JSON formats to IPS, and convert IPS to other standards such as EU-DCC or OMS DDCC.

- **MHD Services:** All the necessary components to implement the MHD services, in particular the ITI 65, ITI 66, ITI 67 and ITI 68 methods to search document bundles, references and obtain documents, will be raised.

- **Web Application:** Corresponds to a web application that works as a client for IPS. It contains an IPS viewer and validator that can work directly with the JSON of the Bundles or connected to a FHIR server.

5. Enabling technical activities

Country Node Configuration

The purpose of this activity is for country teams to deploy local working environments, use IPS tools, DDCC, terminologies and additional services.

- Work environment configuration using Docker
- Installation of HAPI FHIR server.
- Installation and configuration of IPS, DDCC and other modules contained in the Docker.
- Emission testing, transformations and local validation.

Methodology

- Use of LACPASS tools and platform. Docker Compose and associated repository: https://github.com/RACSEL/IPS-national-backend
- Coordination and status in biweekly Regional Technical Committees.
- Training sessions and workshops associated with LACPASS tools.
- Discreet communication and resolution of doubts via Slack: racselworkspace.slack.com
- Participating country teams composed of Ministries of Health and e-Government, immunization departments or entities associated with the project themes.
- LACPASS technical support team to accompany the countries.

6. Detail of Use Cases

6.1. (M) Initialize Country Node

To initialize the Country Node, the following actions must be performed:

1. Generate public and private key pair

The pair of public and private keys that will be used to sign the system's transactions and certificates must be generated. These keys must comply with the security levels defined by each country. The public key must be uploaded to the public key repository of the Regional Node.

2. To raise the services of the Country Node

The official repository of the country node must be cloned and made available at the following link: https://github.com/RACSEL/IPS-national-backend, then the available services must be uploaded in the docker-compose file included in the repository following the instructions of the repository README. Countries that already have their own FHIR or terminology server services can use their own services.

3. Implement service to generate IPS

The necessary activities must be performed and implemented to connect the services or local databases with the FHIR server to upload patient information in order to generate IPS documents.

4. Register the server

To register the server, the LACPass technical team must be informed of the address of the FHIR server in order to incorporate it into the Regional Node and the broadcast service. The technical team will test that the server is available to receive requests so it must have public output. The server must be configured so that the Regional Node can communicate and send transactions.

In addition, the technical team must be provided with the public key for signing the DDCC certificates to be incorporated into the LACPass public key exchange gateway.

System security will be handled by authorizing the server to communicate with the Regional Node and the origins of each country. It is recommended that the FHIR server only supports GET queries from external sources.

6.2. (M) Persist and Validate Test Patient IPS: International Patient Summary

This use case has 3 associated sub-cases to test within the connectathon. The purpose of the use case is the generation and persistence of an IPS summary and the consultation of other care summaries within the different nodes that are part of the connectathon.

6.2.1. Generate and persist an IPS

Country teams must generate an IPS Summary document, according to the implementation guide, available at: http://lacpass.create.cl:8089/index and include at least the following standardized elements/fields:

A nivel de contexto:	Secciones requeridas para la Conectatón:
• Patient - Subject • Provider - Organization • Professional - Practitioner	• Medications • Allergies • Diagnostics • Immunizations..

Once the message has been constructed according to the guide, it must be executed to achieve its persistence in the local country node, using the specifications of the MHD profile, in particular:

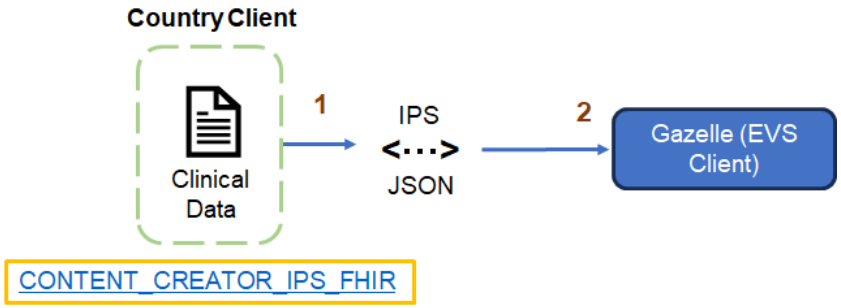
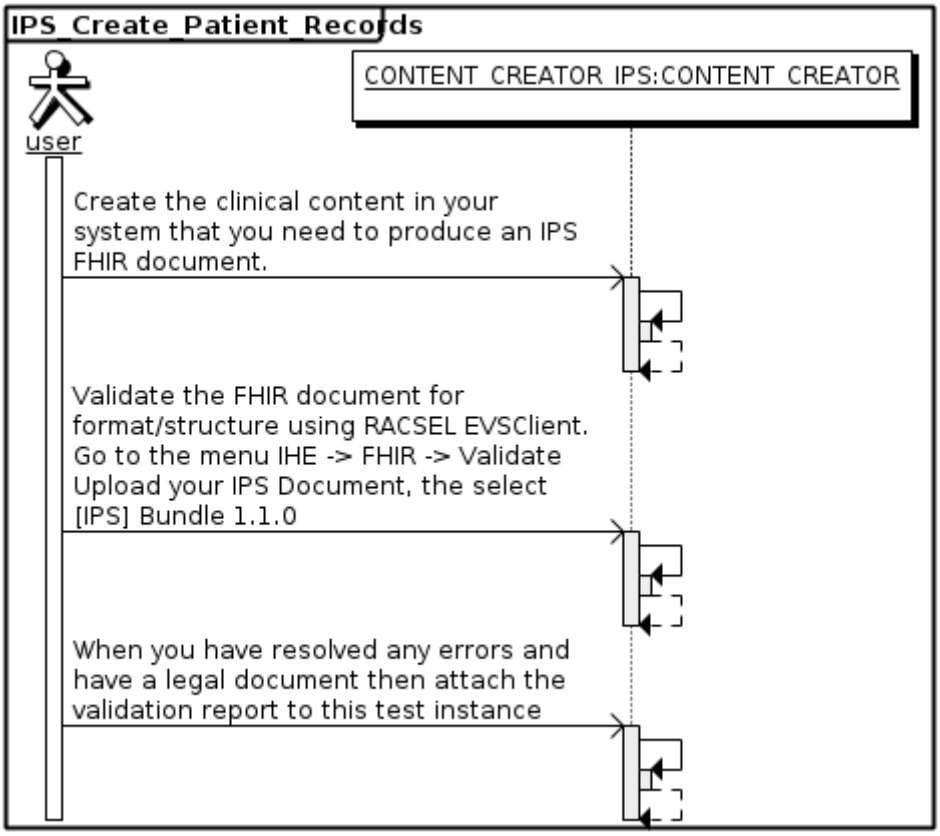


Fig.03: Process diagram of IPS-LAC validation through EVS Client

For all MHD profile transactions defined for these proofs of concept, previously validated IPS will be used as described in the previous figure and detailed in the following step-by-step:

1. Create the clinical content in your system that you need to produce an IPS FHIR document.
2. Validate the FHIR document for format/structure using RACSEL EVSClient
3. Go to RACSEL EVSClient https://gazelle.racsel.org/EVSClient/home.seam
4. Log in with your Gazelle account
5. Go to the menu IHE -> FHIR -> Validate
6. Upload your IPS Document, the select **[IPS] Bundle 1.1.0** as the Model Based Validation
7. Click on Validate
8. When you have resolved any errors and have a legal document then attach the validation report to this test instance.
9. Mark the test as "To Be Verified"



iFig.04: Sequence diagram of IPS-LAC validation using EVS Client

Once a valid IPS is available, it must be executed to achieve its persistence in the local country node, using the specifications of the MHD profile, in particular ITI-65. For this transaction, two similar tests of different difficulty are proposed. POST of IPS bundle to the mediator and ITI-65 transaction to the FHIR server, figures 04 and 05 respectively.

The first test is defined as basic test and consists in performing a POST transaction to provide a Document Bundle through the mediator, according to figure 05 below:

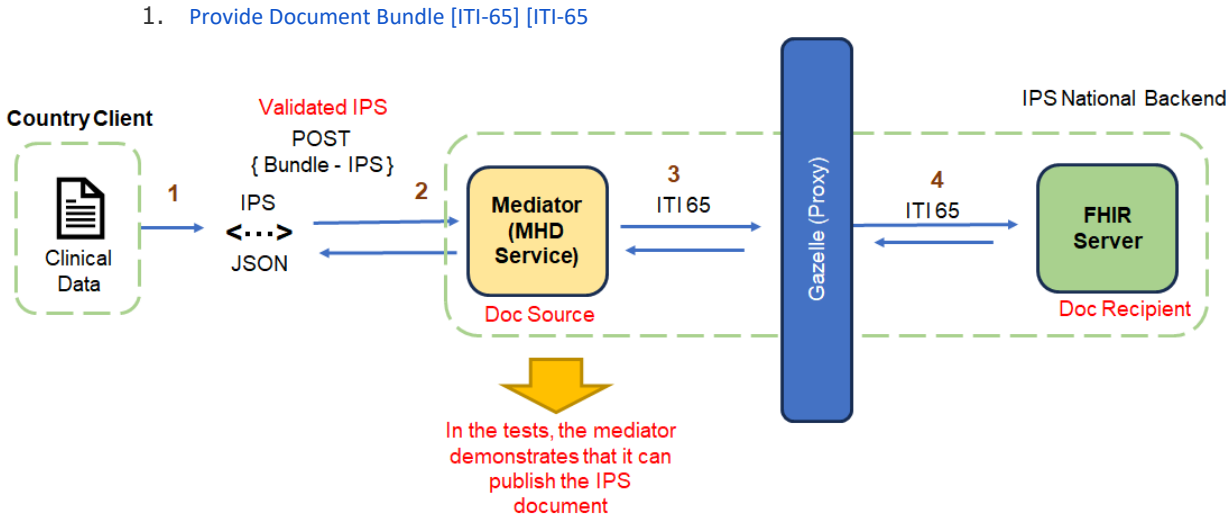


Fig.05: Transactional diagram for ITI 65 Provide document Bundle with mediator..

The objective of this test is for the country client to be able to send a validated IPS document to the mediator and for the mediator to perform the ITI-65 transaction to register the IPS document in the FHIR server.

This message involves a request from a document source (Country Mediator) to transfer a FHIR document to a document recipient (Country FHIR Server).

The Gazelle proxy intercepts the request sent by the mediator. It then transfers the message to the FHIR server. In turn, the proxy intercepts the response message from the FHIR Server and transfers it to the Mediator. Both the request and response messages are accessible from the Gazelle proxy, and the Gazelle proxy will invoke MHD validators in EVSClient.

1. The country client makes a post of the validated IPS bundle to the Mediator. Please add the IPS Bundle to the logs

2. Send the Bundle containing the Patient Summary to the Gazelle proxy, performing a POST to the / endpoint using the [ITI-65] transaction.

3. Search for the request message you send from the SUT (Document Source) to the SUT (Document Recipient) and add validation link from EVSClient - Select the validator [MHD] ITI-65 Provide Document Bundle - Minimal Metadata

4. If the Document Recipient has successfully accepted the submission, it responds with bundle that contains one entry for each resource received from the Doc Source, and an HTTP response code 200 (OK).

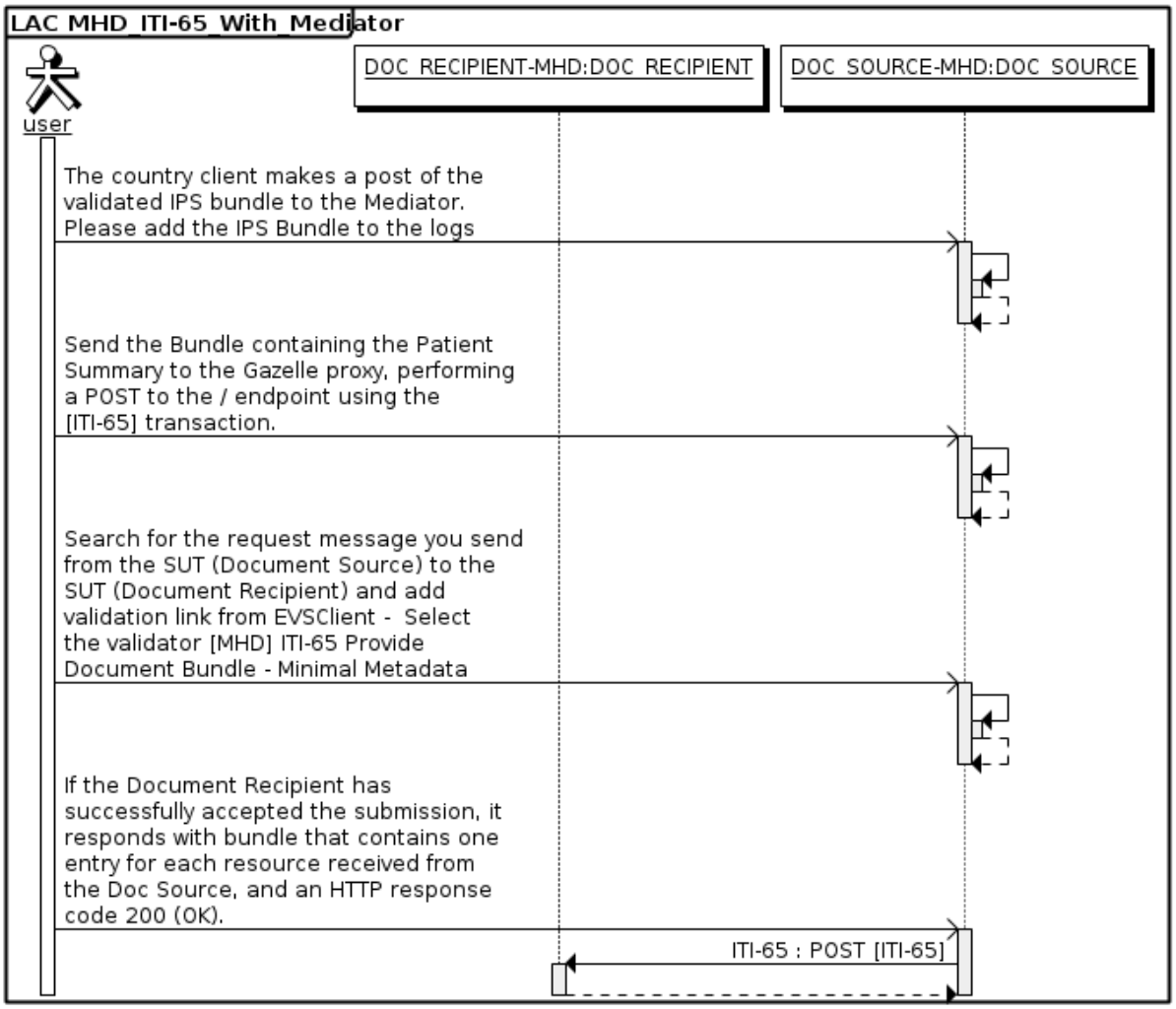


Fig.06: Transactional diagram for ITI 65 Provide document Bundle with mediator.

The next level of difficulty for this test is defined as advanced test and consists of performing a POST transaction to provide a Document Bundle [ITI-65] directly to the FHIR server.

This message involves a request from a document source to transfer a FHIR document to a document recipient. The request is received by a document recipient that stores the received FHIR document and returns an HTTP response code.

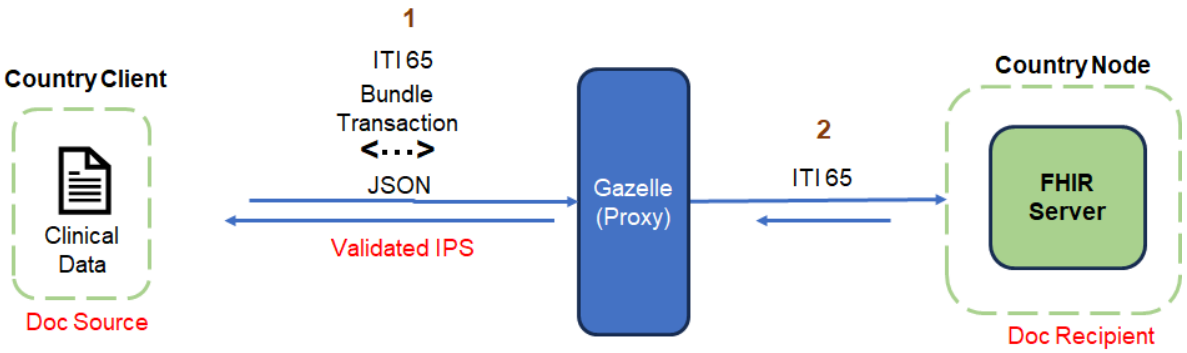


Fig.07: Transactional diagram for ITI 65 Provide document Bundle without mediator

1. See the instructions in the Test Scenario and perform any preparatory activities if applicable.

2. Send the Bundle containing the Patient Summary from your Client SUT to the Gazelle proxy, performing a POST to the / endpoint using the [ITI-65] transaction.

3. If the Document Recipient successfully accepted the submission, it responds with bundle that contains one entry for each resource received from the Doc Source, and an HTTP response code 200 (OK).

4. Search for the request message you send from the SUT (Document Source) to the FHIR Server (Document Recipient) and add validation link from EVSClient - Select the validator [MHD] ITI-65 Provide Document Bundle - Minimal Metadata

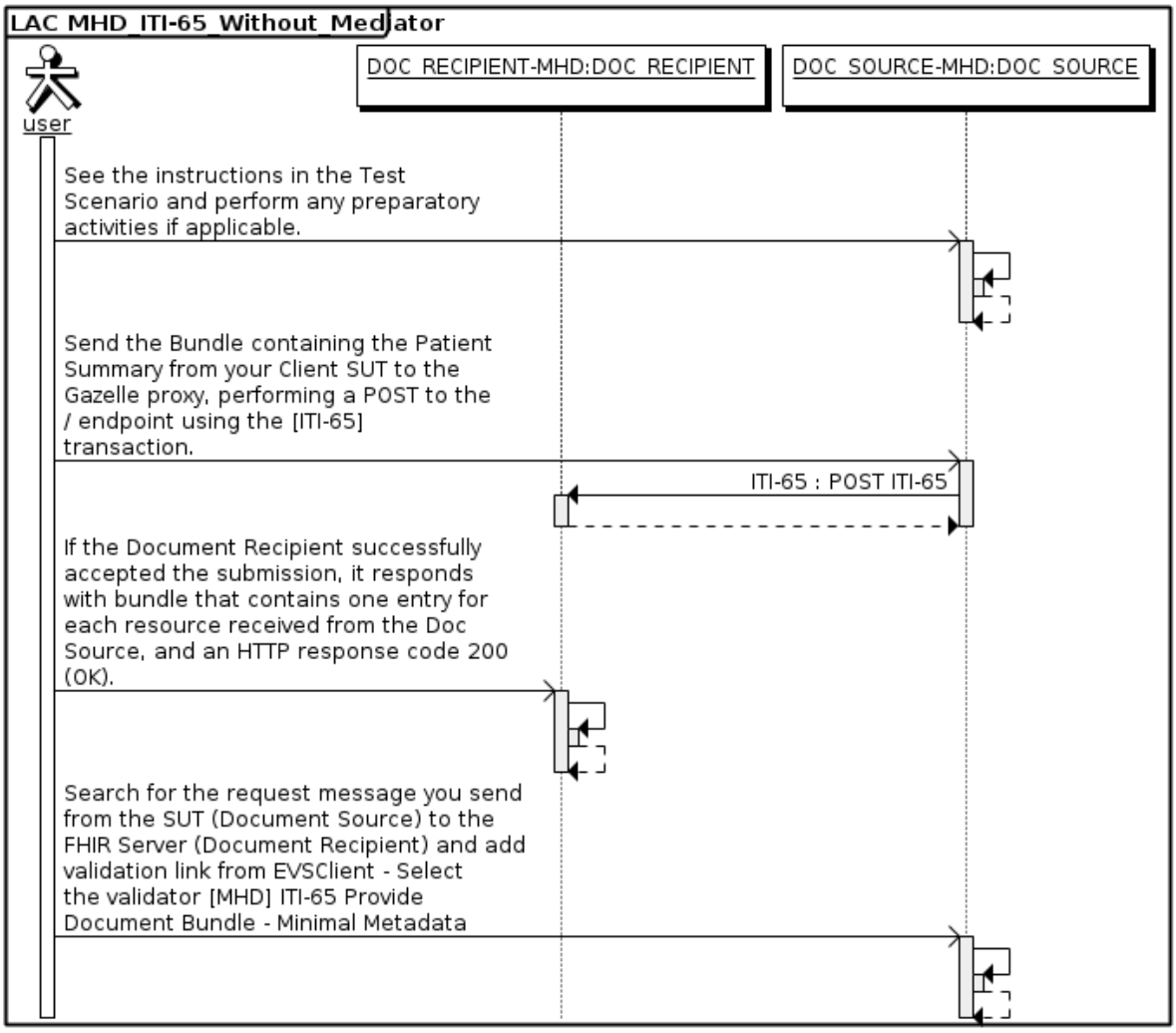


Fig.08: Transactional diagram for ITI 65 Provide document Bundle without mediator.

6.2.2. Search IPS on network nodes

This sub-case of use interacts with the LACPASS network, requesting the regional node to broadcast to the country nodes in search of clinical data for a particular patient.

It is based on the ITI-67 transaction, whereby, given a patient identifier - which may be a National ID or passport number - the regional node is asked if there is information in the network associated with clinical documents for the identifier consulted:

Find Document References [ITI-67]

Request ejemplo: GET{{broadcast_server}}/fhir/DocumentReference/?patient.identifier=CL/15829877-5&_format=json&status=current

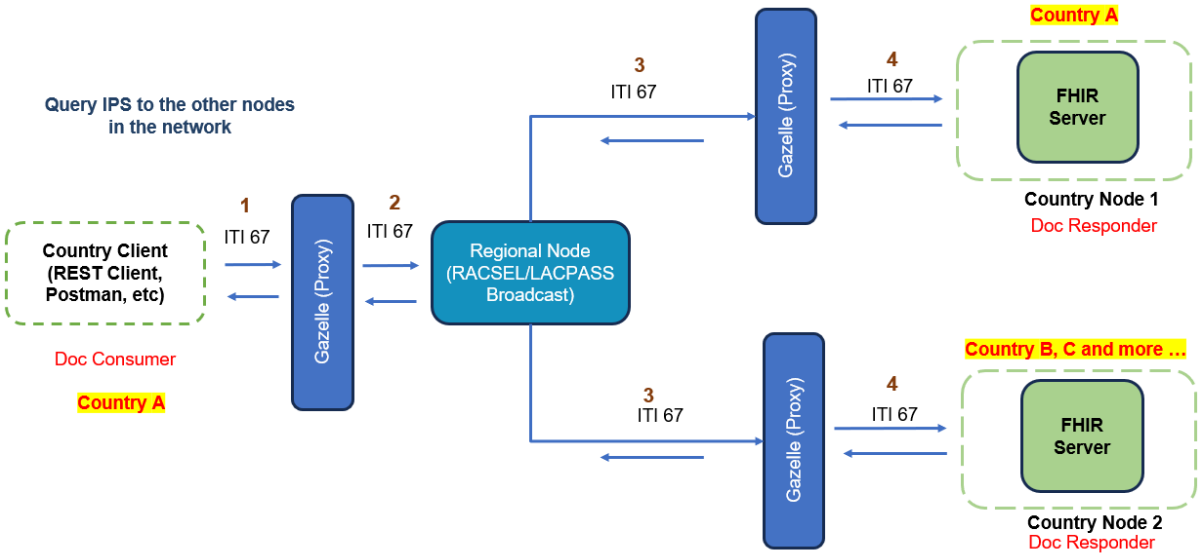


Fig.09: Transaction diagram for ITI 67 Find document Reference.

1. Send the query from your SUT to the Gazelle proxy, performing a GET to the /DocumentReference endpoint or a POST to the /DocumentReference/_search endpoint using the [ITI-67] transaction.

2. If the Find Document References message is processed successfully, whether or not any DocumentReference Resources are found, the HTTP status code shall be 200. The Find Document References Response message shall be a Bundle Resource containing zero or more DocumentReference Resources. If the Document Responder is sending warnings, the Bundle Resource shall also contain an OperationOutcome Resource that contains those warnings.

3. Search for the response message you send from the Document Responder to the Document Consumer and add validation link from EVSClient - Select the validator [MHD] ITI-67 Find Document References Response Message

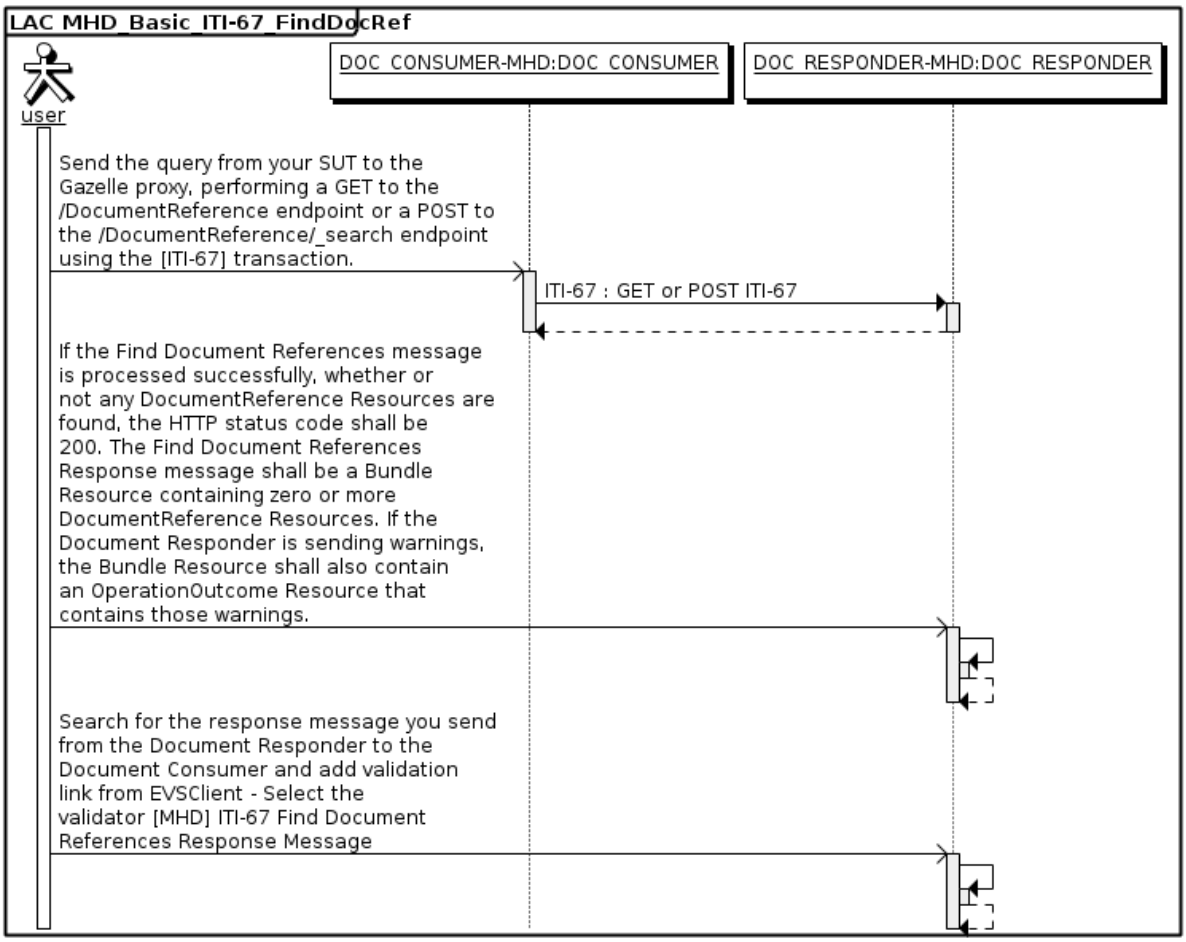


Fig.10: Transaction diagram for ITI 67 Find document Reference.

6.2.3. Retrieve IPS

This transaction implements accessing a specific IPS document selected from the previous query subset. This transaction is triggered directly to the local node of interest, assuming that the previous search was successful.

The following transaction will be used for this purpose:

Retrieve Document [ITI-68]

Request ejemplo: GET http://lacpass.create.cl:8080/fhir/Bundle/f25f53b2-99e9-4b48-98b5-682be348f9cc

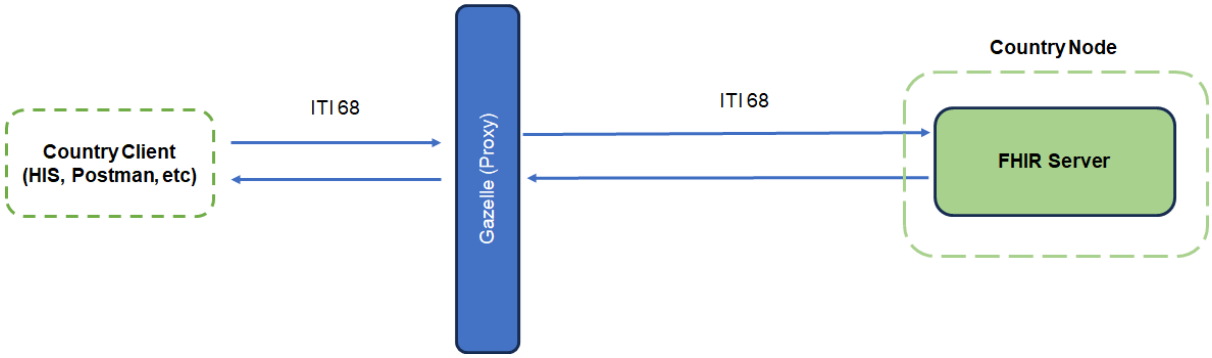


Fig.11: Transaction diagram for ITI 68 Retrieve document.

1. Send the request from your SUT to the Gazelle proxy using a [ITI-68] transaction, performing a GET to the Patient Summary reference URL.

2. When the requested document is returned, the Document Responder shall respond with HTTP Status Code 200 (OK). Upon error, the Document Responder should complement the returned error code with a human readable description of the error condition.

6.3. (M) TRACK 2A: DDCC/DDVC Certificate Generation and Verification

The purpose of the use case is the correct issuance and verification of vaccination certificates for Covid and Non-Covid according to the WHO-DDCC profile. The track considers to generate certificates for non-covid vaccines in an experimental way from a limited white list of vaccines for Yellow Fever, Polio and Measles. The generation of these certificates depends on the data contained in the immunization section of the previously generated IPS.

- **(M)** ***Onboard WHO Trustlist / LACPASS Gateway***

The onboarding process for track 2A requires the generation and sharing of public keys according to x509 standard for the signature and verification of vaccination certificates. This key must be issued by a valid certificate authority. For the purposes of the LACPASS Connectathon, valid keys will be generated by t-systems/WHO and distributed to Connectathon participants. The delivered key must be stored in the cert-data folder of the LACPASS docker for the correct functioning of the vaccination certificate generation.

- **(M)** ***IPS with various pathogens as prerequisite (track 1.a)***

For the correct generation of several vaccination certificates, it is a prerequisite to have a previously generated IPS (in track 1) containing 2 or more immunizations, ideally of at least 2 different pathogens, covid and non-covid and the corresponding Public Key according to the x509 standard available on LACPASS Connectathon defined gateways.

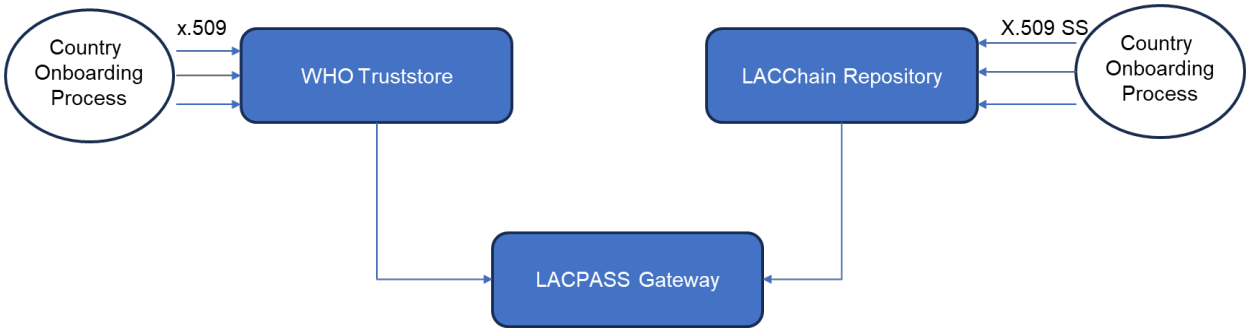


Fig.13: Gateway interaction and synchronization diagram for Conectaton LACPASS

- **(M) *Generation of DDCC/DDVC certificates***

It consists of the generation of DDCC/DDVC vaccination certificates from immunization data obtained from the definition of the IPS-LACPASS implementation guide, in particular from the IPS Immunization resource and other resources that can provide information to complete the data defined in the DDCC QuestionnaireResponse, this has an additional component since it requires transformations of some elements related to Value Sets that it is necessary to have beforehand.

To generate these certificates the IPS mediator is used (contained in the LACPASS docker) where a FHIR operation called $ddcc is implemented, whose function is to transform the IPS packages into DDCC/DDVC documents. For this operation to work, it is mandatory that the stored IPSs have at least one Immunization resource.

Request: GET 'http://localhost:3000/fhir/Bundle/fb06a834-6b55-4ac3-a856-82489eb4d69d/$ddcc'

Where fb06a834-6b55-4ac3-a856-82489eb4d69d is the id of the IPS Package. This endpoint returns the DDCC Packet associated with the requested IPS.

This transformation retrieves a previously stored IPS and checks if the Immunization resource is present. The process extracts the IPS information to build the QuestionnarieResponse with the DDCC structure. This QuestionnarieResponse is sent to the DDCC module to generate the document, according to the following image:

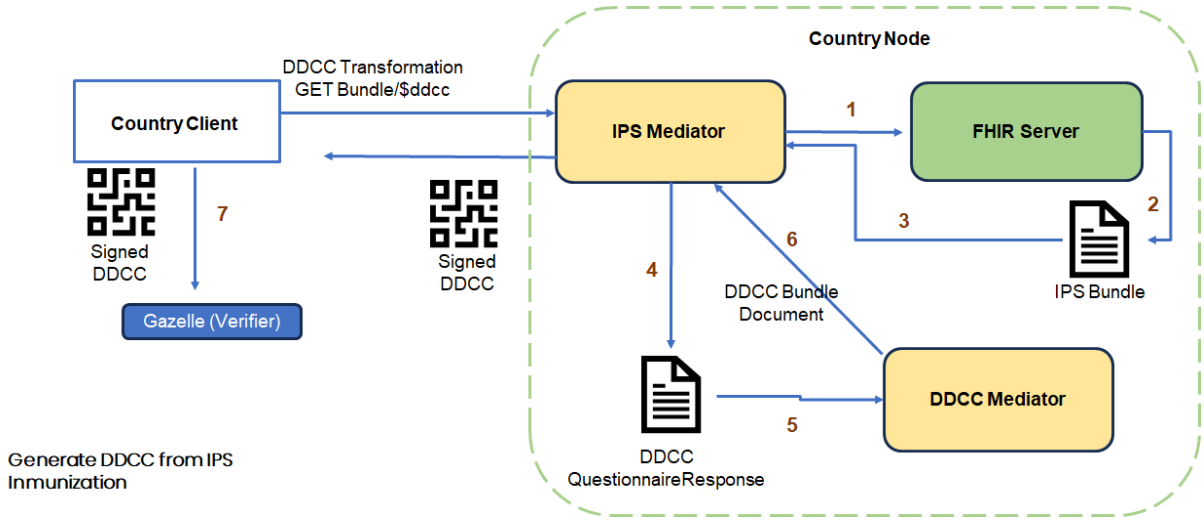


Fig.14: Transaction diagram for DDCC generation from IPS Immunization..

Optionally, if the IPS has more than one Immunization resource, you can pass the query argument immunizationId to specify the id of the Immunization resource to transform. For example.

Request: GET 'http://localhost:3000/fhir/Bundle/fb06a834-6b55-4ac3-a856-82489eb4d69d/$ddcc?immunizationId=6fef12e7-64ad-4792-b2ad-5d6b699588fc'

- **(M)** ***Verification of certificates with U-WHO No p2p and P2P***

1. Once the DDCC/DDVC is generated, it is validated in the universal verifier available in gazelle. There are two types of verifications: NoP2P and P2P.

2. For the NoP2P test it is enough to load the certificates in the universal verifier available in gazelle and obtain the results.

3. For the P2P test it is required to make available in gazelle the generated certificates for others to validate, in the same way it is requested to validate the third party Certificates available for each country. This validation must be done 3 times depending on the number of participating countries.

4. Each type of NoP2P and P2P test will be repeated for a COVID (DDCC) and a NO-COVID (DDVC) certificate.

- **(O)** ***Verification of certificates with U-LACChain No p2p***

Additionally it is possible to test the verification of DDCC/DDVC certificates through the LACCHAIN verifier, just upload the certificates in the universal verifier available at URL LACCHAIN and get the results.