



# Progress Report

*Component 1 LACPASS*

RED AMERICANA  
DE COOPERACION  
SOBRE SALUD  
ELECTRONICA



Introduction	3
Evolution of the Regional Public Goods	4
Conectaton LACPASS	11
Goals	11
Mission	11
Conectaton Progress	13
Test Cases	15
Results	16
Conectaton LACPASS Survey	21
Conectaton Conclusions	27
Lessons Learned	28
Annexes	29
Annex 1- LACPASS Technical Documentation	29
Introduction	29
Architecture	30
Security and Encryption Keys	32
Implementation	33
Verification Mobile Apps	47
Frequent questions	53
Annex 2- Conectaton LACPASS Test Cases	55
Test Cases	55
Test Instance Execution Guide	58

## Introduction

The changes caused by the COVID-19 pandemic accelerated many processes, mainly those involved in Healthcare Information Systems; these had to be changed swiftly because the method in which medical attention was provided had also had to change.

In addition, and because of the amount of information generated by the need to perform COVID-19 tests, the need for vaccinations caused for countries themselves to have to organize the information so it could be quickly accessed by both their inhabitants and by healthcare authorities.

Subsequently, the vaccination progress showed that the pandemic was starting to be manageable because both the number of cases and the mortality rate decreased due to the quick vaccination campaigns launched in all countries. It was then possible to start thinking about opening borders while respecting the healthcare guidelines imposed by the different countries. The need for the use of COVID-19 certificates arose as a way to guarantee an individual's health condition.

All countries began with the digitization challenge, which allowed for both individuals and Healthcare Institutions to quickly access information. Many countries started this at a country level, allowing individuals to take part in several activities through the use of these digital certificates. Later on, they started including certificates as requirements for cross-border travels.

The European pioneered the implementation of certificates for cross-border traveling with all member countries verifying and validating these certificates. This meant that the borders for EU countries could be opened while still guaranteeing the healthcare situation of anyone traveling from one country to the other. Later on, the EU allowed countries that did not belong to the EU, but which met EU-DCC requirements, to move freely within the EU.

The model implemented by the EU generated the possibility of implementing it in Latin America and the Caribbean<sup>1</sup>. After a lot of hard work, the first Conectaton for Latin America and the Caribbean was held in Santiago de Chile.

---

<sup>1</sup> See Annex 1- Technical Documentation

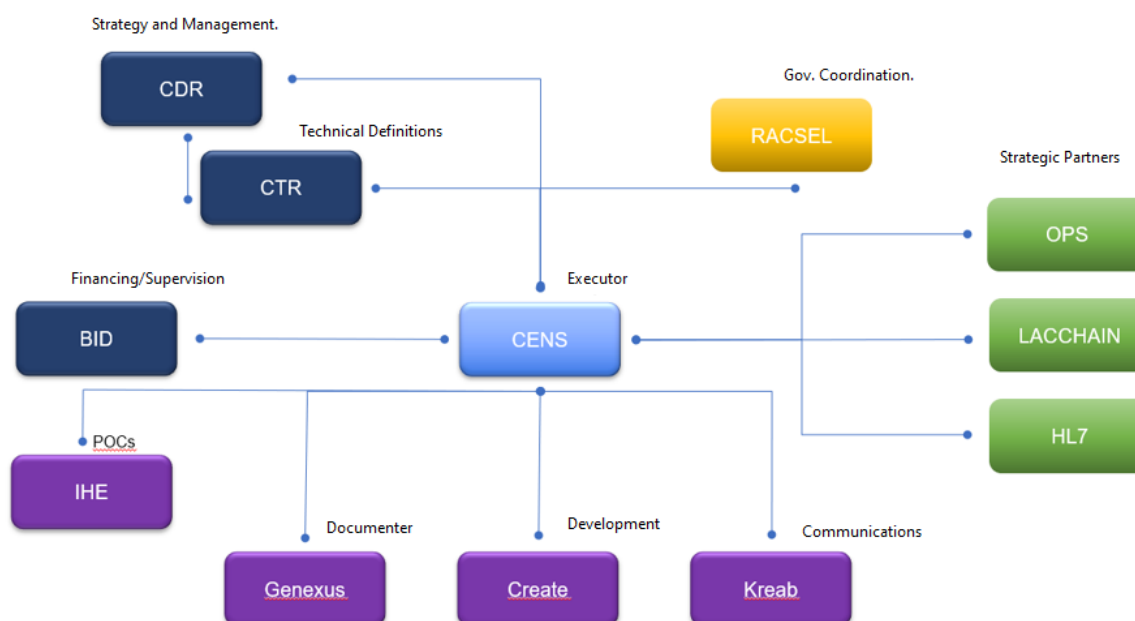
## Evolution of the Regional Public Goods

The aim of the Regional Public Goods (RPG) is to strengthen the ability of the countries in Latin America and the Caribbean to cope with the effects of COVID-19, while also fostering a digital transformation in the healthcare industry within the region.

The RPG aims to strengthen the exchange of healthcare information within and between countries in the region through the implementation of 3 components distributed in 3 years:

- To increase the levels of interoperability for the exchange of healthcare clinical data.
- To exchange data to monitor the epidemic and the healthcare situation both at a national and a regional level.
- To establish the guidelines and directives required for the sustainable development of Telehealth or Telemedicine.

The structure of RPG – Component 1 is the following:



The RPG provides a governance in which we find several different actors with different roles and functions. It is formed by a Regional Directive Committee (RDC), an implementation agency, which corresponds to the National Centre for Healthcare Information Systems (“CENS” for its acronym in Spanish). The Inter-American Development Bank (IADB) and other strategic partners oversee the execution of the project.

In relation to the governance mechanisms, the Regional Directive Committee (RDC) is responsible for:

- Making strategic decisions.
- Monitoring the project's progress and results.
- Ensuring the quality and use of products.
- Deciding on the incorporation of any new countries.

The technical committee, on the other hand, is responsible for:

- The definition of the standards and the architecture.
- The trust framework.

At the start of the process, the following countries took part in the process. We will describe their initial situation hereunder:

- Argentina
- Chile
- Colombia
- Paraguay
- Suriname
- Uruguay

When the process started, a survey was carried out among all participating countries covering three main goals:

- Understanding: to generate a direct interaction between each of the participating countries, which made it possible to understand the technical level each country possessed.
- Expectations: to know the expectations each country had with regards to their participation in the project.
- Dialogue: to establish a personalized dialogue with each of their teams to bridge any gaps and existing requirements for each of the countries.

As a starting point for the digitization process within the region, an interview was carried out with expert representatives for each country to learn about their current status. The information that was gathered was grouped into three different categories; a scale was created to group results into three groups: High, Medium, and Low.

The categories in which answers were grouped were:

- Project vision and participation: the aim of this category was to understand the expectations for the project and the deadlines involved, what the level of Institutional participation would be, and the level of the participating human resources.
- Status of their current vaccination system: the aim was to understand the maturity of the national vaccination registry the country already had, whether they were using standards such as FHIR or CIE-11, and whether the vaccination certificates were digitally signed.

- Discovery of any gaps and/or needs regarding IHE Profiles: the human capital in digital healthcare and their architecture and infrastructure.

Following are the results of the interviews for each of the countries:

- Argentina: in the interview, they declared that they were aligned with the vision and expectations for the project. The human resources had a high technical level, but the commitment of the resources was very complex. They were not currently using CIE-11, and they had a centralized vaccination registry which was updated with FHIR. Certificates were digitally signed.
- Chile: in the interview, they had expectations and deadlines which were aligned with the project. At that time, they were defining the formalization of the participants. They had a medium technical level, a single registry set up with FHIR and digital signatures, and they were not using CIE-11.
- Paraguay: the expectations for the project and their deadlines were adequate, but the commitment of resources was limited. They had a medium technical level, a single registry set up with FHIR and digital signatures and had no CIE-11.
- Suriname: the expectations and deadlines for the project were adequate and had a great deal of commitment and participation aligned with the project. They were currently implementing DHIS2 at a national level aiming at using the standards. They needed FHIR, digital signatures, and CIE-11 development.
- Uruguay: they had a vision and expectations aligned with the projects, the support required for RPG, a high technical level, mapping from CDA3 to FHIR, and were not using CIE-11. They raised doubts regarding the architecture and the infrastructure needed to perform the proofs of concept.

When drafting a global summary of the responses obtained from the interviews for each of the categories, we found the following status:

- Project vision and participation: we found that the expectations of all of the interviewed countries were aligned with the project and the deadlines. In addition, there was a high degree of participation commitment. However, this was during the formalization period: an exclusive commitment to the project was complex.
- Status of their current vaccination system: there were different levels of maturity for vaccination registries at a national level for each of the countries. In relation to standards, we found that FHIR should be implemented in all countries with different efforts involved for each one of them. The outlook for implementing CIE-11 was much more complex. All countries had experience with digital signatures and certifying authorities.
- Discovery of any gaps and/or needs: IHE profiles were present in all countries with different levels of adoption. The human capital would need to strengthen their digital healthcare, and there were concerns regarding the available architecture.

These interviews allowed us to learn more about the situation of the healthcare information systems for each of the countries, which are crucial to the digital transformation process for the region.

Likewise, the Technical Committee came up with two groups with the aim to define two fundamental aspects. Following is a description of the discussions that were carried out for each of the technical groups.

It was crucial for these groups to cover three important items for the development of the project: Architecture and Standards, Trust Frameworks, and the privacy and security of the information to be exchanged.

The group carried out a discussion about the Data Model, where the following topics were discussed:

### Header

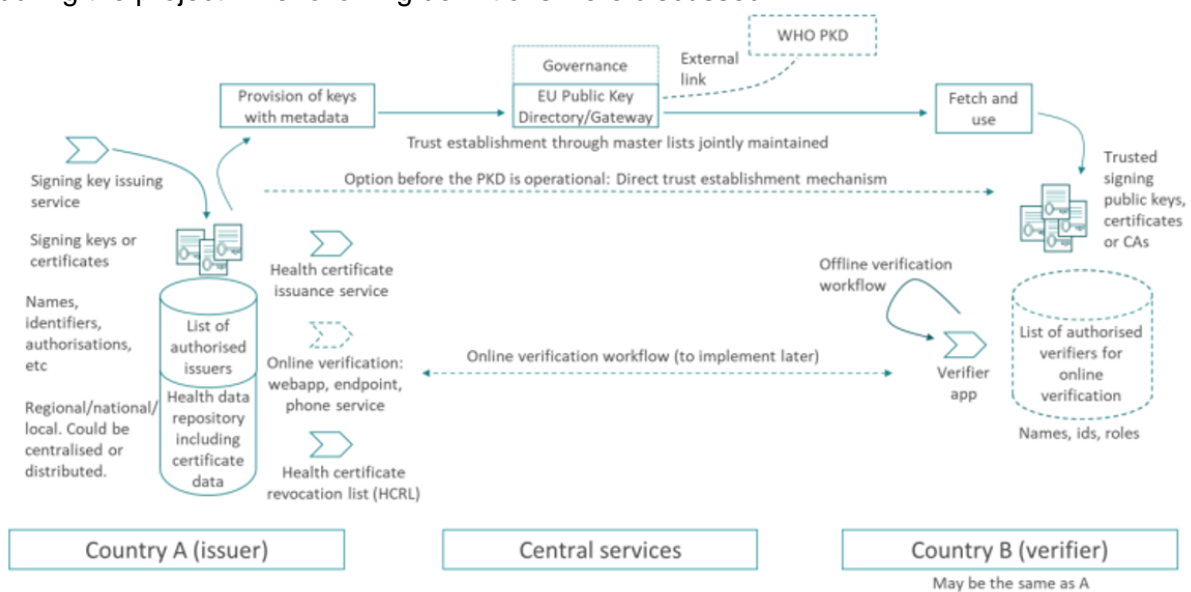
Data element	Description	Requirement status	Data type	Preferred code set
<b>Name</b>	The full name of the vaccinated person	Required	String	Not applicable
<b>Date of birth</b>	The individual's date of birth (DOB) if known. If unknown, use given DOB for administrative purposes. The full format of DD MM YYYY is required if known.	Required - If known	Date	Not applicable
<b>Unique identifier</b>	Unique identifier for the vaccinated person, according to the policies applicable to each country. There can be more than one unique identifier used to link records. (e.g. national ID, health ID, immunization information system ID, medical record ID).	Optional - Recommended	ID	Not applicable
<b>Sex</b>	Documentation of a specific instance of sex information for the vaccinated person.	Optional - Recommended	Coding	As defined by Member State

### Data Elements

Data element	Description	Requirement status	Data type	Preferred code set
<b>Vaccine or prophylaxis</b>	Generic description of the vaccine or vaccine sub-type. e.g. Covid-19 mRNA vaccine, HPV vaccine.	Required	Coding	ICD-11
<b>Vaccine brand</b>	The brand or trade name used to refer to the vaccine received.	Required	Coding	As defined by Member State
<b>Vaccine manufacturer</b>	Name of the manufacturer of the vaccine received. e.g. Serum institute of India, AstraZeneca. <i>If the vaccine manufacturer is unknown, vaccine market authorization holder is REQUIRED.</i>	Required – Conditional	Coding	As defined by Member State
<b>Vaccine market authorization holder</b>	Name of the market authorization holder of the vaccine received. <i>If vaccine market authorization holder is unknown, then vaccine manufacturer is REQUIRED.</i>	Required – Conditional	Coding	As defined by Member State
<b>Vaccine batch number</b>	Batch number or lot number of the vaccine.	Required	String	Not applicable
<b>Date of vaccination</b>	Date in which the vaccine was provided.	Required	Date	Not applicable
<b>Dose number</b>	Vaccine dose number.	Required	Integer quantity	Not applicable
<b>Country of vaccination</b>	The country in which the individual has been vaccinated.	Required	Coding	ISO 3166
<b>Administering centre</b>	The name or identifier of the vaccination facility responsible for providing the vaccination.	Required	Coding	As defined by Member State
<b>Signature of health worker</b>	REQUIRED for PAPER vaccination certificates. The health worker who provided the vaccination or the supervising clinician's hand-written signature.	Required – Conditional	Signature	Not applicable
<b>Health worker identification</b>	REQUIRED for DIGITAL vaccination certificates. The unique identifier for the health worker as determined by the Member State. There can be more than one unique identifier used. (e.g. system generated ID, health profession number, cryptographic signature, or any other form of health worker unique identifier). This is to be used in lieu of a paper-based signature.	Required - Conditional	ID	Not applicable
<b>Disease or agent targeted</b>	Name of disease vaccinated against (such as COVID-19)	Optional - Recommended	Coding	ICD-11
<b>Due date of next dose</b>	Date on which the next vaccination should be administered	Optional - Recommended	Date	Not applicable

- Review of the metadata.
- Standards used (FHIR, CIE-11 and SNOMED CT).
- Placement of the Information Model for the DDCC.
- Identifiers, Spanish, list of values and semantics.
- ALC data model.
- Adoption of CIE-11.
- Subsets.
- Guidelines for the technical guide and data model.

The second technical group had a discussion regarding the exchange model to be carried out during the project. The following definitions were discussed:



- Identification of components for the architecture of the information exchange, the security, and the digital signature.
  - Components
  - Security
  - Signature
  - QR Code
  - Technical Guide guidelines for the exchange model.

Another aspect to point out for the project is the defined strategic level, which covered three main aspects:

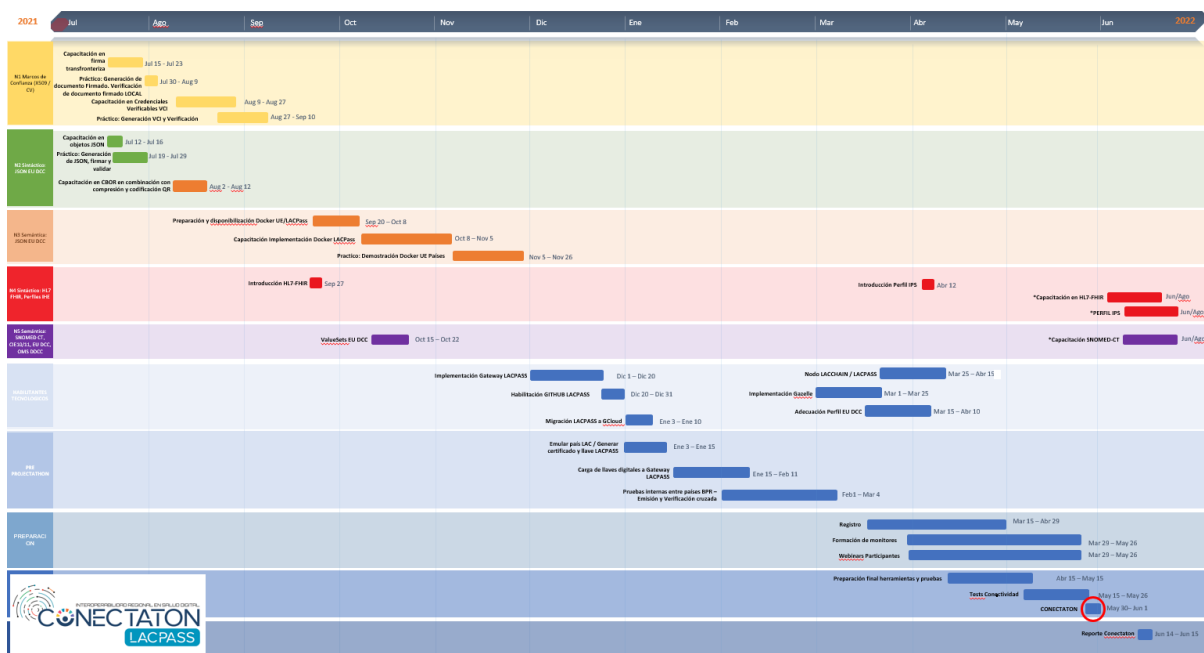
- Standards: to follow the guidelines provided by the WHO, the DDCC, and the EU certificate.
- To align with the strategic plans set forth by the PAHO: implement open digital healthcare and information systems that are sustainable and interoperable.

- Development and skills: to foster the development of skills in order to be able to use data science and emerging technologies for the research, innovation, public policies, and ethical analysis in public healthcare.

These aspects aimed to obtain the following results:

- Standards: to be able to develop a learning and knowledge process linked to the standards required for the data and the trust framework.
- Infrastructure: to implement a regional Gateway.
- Proofs of concept: to implement tests based on digital signature standards.
- Interoperability: to execute a Projectathon which would make it possible to achieve interoperability at a regional level.
- Scalability: to develop technical information with includes the lessons learned in additional to a scalability analysis.

Having said that, the preparation process for the project implied a series of additional activities in which all countries had to be present. To this end, we carried out the planning for the activities and the deadlines that had to be met during the course of the project.



The current plan started in July 2021, with 10 different stages to be met throughout the project. In addition, each of the stages had a list of activities to be carried out.

The 10 stages proposed in the GAM are:

- Level 1, Trust Framework, XS09/CV.
- Level 2, Semantic JSON EU DCC.

- Level 3, Semantic, JSON EU DCC.
- Level 4, Semantic HL7, FHIR, IHE Profiles.
- NS, SNOMED CT Semantic, CIE 10/11, EU DCC, OMS DDCC.
- Technical enablers.
- Pre Projectathon.
- Preparation.
- Projectathon.
- Post Projectathon.

These stages will be carried out between July 2021 and June 2022 approximately. As mentioned above, each of the stages has different activities that must be carried out, which will allow for the goals of the project to be met. Some of the stages include significant milestones within the region.

The training requirements for different topics is always present within these activities because it is crucial to offer the participating countries the most amount of knowledge possible so they can participate in the project to the best of their abilities. These training sessions will include theoretical and practical knowledge which will reinforce the knowledge provided.

Most of the training sessions were carried out between July and November 2021; technical information required for the project was provided, with topics such as Digital Signatures, generation of locally signed documents, JSON elements and JSON generations, CBOR and QR encoding, and HL7, among other trainings.

In September 2021, Docker EU/LACPASS was prepared and made available, with both theoretical and practical trainings, in addition to the EU DCC ValueSets. This was the first important milestone for the project, which happened in December 2021 with the implementation of LACPASS Gateway.

The implementation of the Gateway exhibited the progress of the countries up until that point, and it generated a start of new challenges for the involved countries. Once it was implemented, some related actions were carried out such as the activation of GITHUB LACPASS, and a migration to GCloud together with a simulation and generation of certificates and LACPASS keys. In order to do this, the countries uploaded their digital keys into the Gateway LACPASS in January 2022.

The upload of the keys allowed the countries to perform the required internal issuance and cross-verification tests with other participating countries.

Once the Gateway was implemented, tasks were carried out in relation to the LACCHAIN/LACPASS Nodes, the implementation of Gazelle, and the adjustment of profiles to the EU DCC.

In March 2022, the registration process was started along with the monitor trainings, Webinars, and final preparations, in addition to a connectivity Test before the Conectaton, which took place from May 30<sup>th</sup> to the 1<sup>st</sup> of June 2022.

## Conectaton LACPASS

### Goals

Conectaton is a connectivity marathon between countries to test out the interoperability of Healthcare Information Systems. It is an event where all healthcare organizations can perform connectivity and interoperability tests in a controlled and neutral environment.

The monitors are responsible for executing these tests. They are in charge of the validation and verification activities during the event.

The main and primary goal is to strengthen the ability of countries in Latin America and the Caribbean to cope with the effects of COVID-19 by promoting digital transformation in the healthcare industry and, from there on, to move forward to new technological challenges within the region, and to ensure that at least three countries were able to correctly finish the tests that were set out for the Conectaton.

Through practical and real tests, the intention is to prove that the different information systems owned by the participating countries can exchange, integrate, and cooperatively use the data with the future goal of exchanging healthcare data and telehealth among other countries in the region.

### Mission

To contribute to the fostering and adoption of healthcare information technology, promoting the development of human capital in a collaborative way, and streamlining the innovation ecosystem to improve the healthcare provided to individuals.

For this purpose, three components that needed to be followed were defined:

- Higher levels of interoperability in the exchange of healthcare clinical data: this component was performed in the current Conectaton, which established the

interoperability guidelines for COVID-19 health certificates in Latin America and the Caribbean.

- Exchange data to monitor the epidemic in Public Healthcare at a National and a Regional level.
- To establish the guidelines and directives required for the sustainable development of Telehealth.

## Conectaton Progress

The Conectaton was carried out from the 30<sup>th</sup> of May to the 1<sup>st</sup> of June in Santiago de Chile. The LACPASS project (See Annex 1) is an initiative of the American Cooperation Network for Electronic Health in Latin America and the Caribbean (“RACSEL” for its acronym in Spanish), which is sponsored by the Inter-American Development Bank (IADB) and executed by the National Centre for Healthcare Information Systems (“CENS” for its acronym in Spanish), who provide this public good.

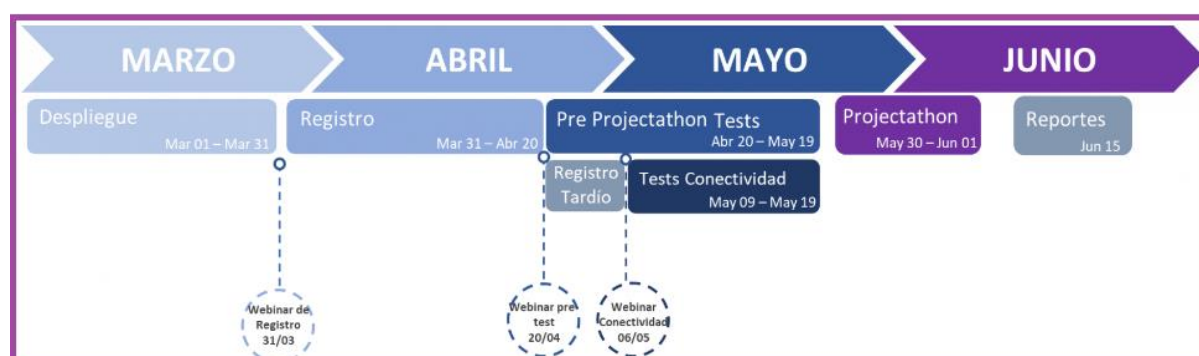
LACPASS is based on the EU Digital Green Certificates (EU DGC), an open-source repository used by countries that belong to the EU. It is also available in different languages for accessibility purposes. By connecting all interested countries to LACPASS, it is possible to use this technology to connect to the EU DGC.

It is for this reason that the LACPASS project allows for certificates issued by the country of residence for cross-border travels to be verified in any of the countries belonging to the project.

The following countries participated in the event: Chile, Colombia, Ecuador, El Salvador, Paraguay, Peru, Suriname, and Uruguay. The countries observing Conectaton were Bolivia and Costa Rica.

In order to be able to hold the Conectaton, a Projectathon schedule was carried out where the participating countries had to go through several stages to be able to finally participate in the Conectaton. It should be noted that Argentina is a member of the public good but did not participate in the Conectaton.

A Projectathon is a one-on-one testing event where the same tools used in a Conectaton are used to allow for the testing of different IHE (Integrating the Healthcare Enterprise) profiles. This aims to reduce any existing risks during the implementation process, because the necessary tests have been performed beforehand.



The Projectathon had the following stages:

- Registration: a process in which anyone wishing to participate needs to complete the registration process.
- Pre-Projectathon Tests: the period in which test are performed with the goal of becoming familiar with the different tools.
- Connectivity: the process through which the connectivity is verified; whether or not the system is ready for real tests to be performed. The monitor is the one confirming whether or not the test was successful.

The monitors are responsible for verifying and rating each of the tests performed, and they determine whether or not the tests performed as expected.

The tool used to manage the interoperability tests was Gazelle (<https://gazelle.racsel.org/>). This website includes all of the technical information required to perform the tests.

During the first two days, connectivity tests were performed for each of the countries. The monitor was responsible for evaluating the progress of these tests and to finally validate whether or not they were completed successfully.

The tests performed by each of the participating countries were related to the generation, issuance, validation of the certificates, and the exchange of certificates between participants. The document with the tests that were performed can be found in Annex 2 of this document.

The following is a description of the tests that were performed, and the results obtained by each of the participants.

## Test Cases

The test cases<sup>2</sup> are the technical activities which make it possible to prove that it is viable for the different healthcare information systems owned by the participating countries to access, exchange, integrate, and cooperatively use the data associated with COVID-19 certificates through the use of LACPASS services defined by the guidelines set forth by the EU-DCC and the IHE Gazelle.

All participants in Conectaton must be able to:

- Create and issue COVID-19 certificates according to the definition carried out by the EU-DCC.
- Validate the certificates issued within the country using the Gazelle platform.
- Verify COVID-19 certificates issued by other participating countries.

All participants will evaluate four levels of test fulfillment:

- Level 1 – Activation: the correct configuration of the trust frameworks, the successful upload and download of the public keys for the validation of COVID-19 certificates.
- Level 2 – Issuance: the successful generation and issuance of COVID-19 certificates from each of the participating systems.
- Level 3 – Verification: the successful verification via the Gazelle platform of COVID-19 certificates issued by each of the participating countries.
- Level 4 – Validation: peer validation of COVID-19 certificates issued by each country. This test case is repeated N times for each participant performing the peer validation.

The technical details for the tests can be viewed in the Conectaton LACPASS Test Case document located in Annex 2.

---

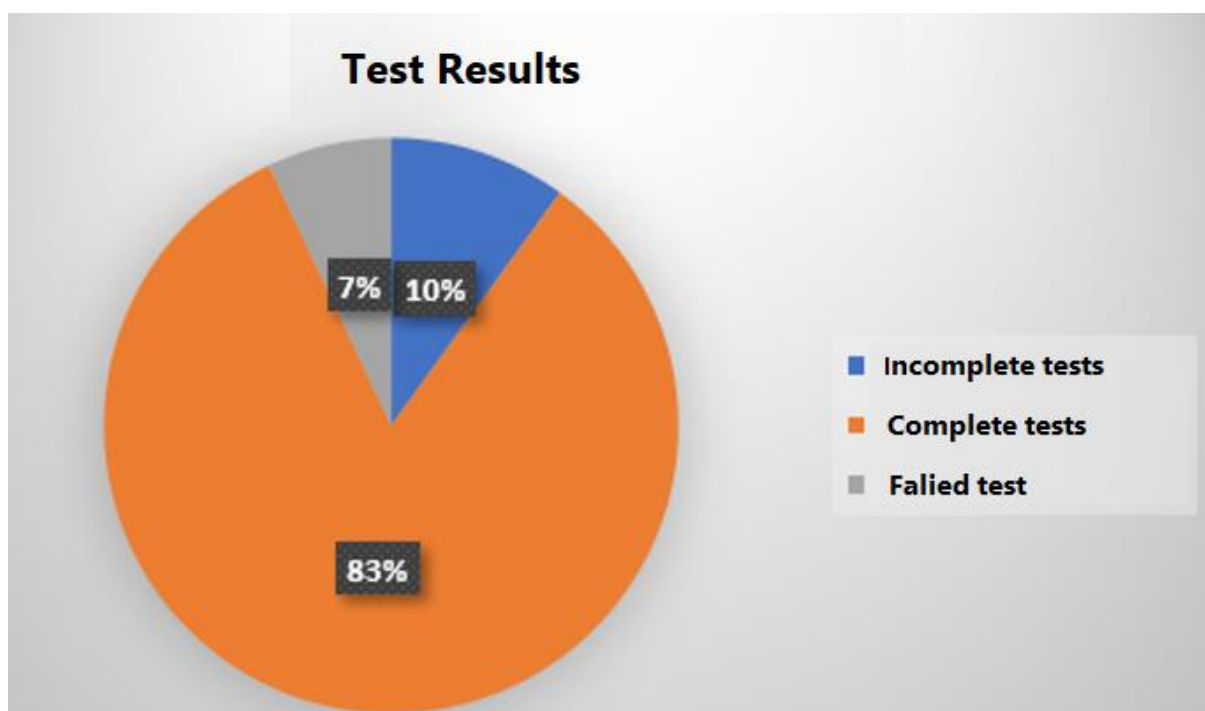
<sup>2</sup> See Test Case Annex

## Results

After two days of tests between participating countries, the following data was obtained, as detailed below:

During the Conectaton event, a grand total of 83 tests were performed with the following results:

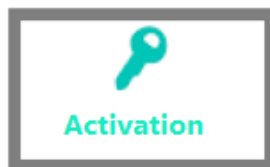
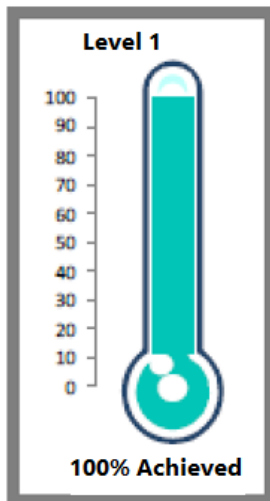
- 83% of the tests were completed successfully (68 tests).
- 10% could not be completed successfully (8 tests).
- 7% of the tests failed (7 tests).



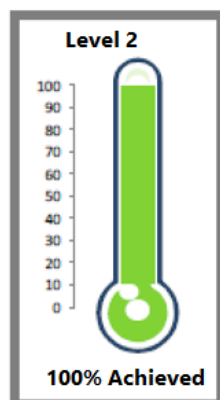
It is important to point out that the tests had to be completed within a predefined timeframe, so any tests performed successfully outside of the timeframe were not validated as successfully completed.

In the case of tests that could not be completed successfully due to connectivity issues, these were caused by an overload of devices connecting at the same time, which generated network dropouts.

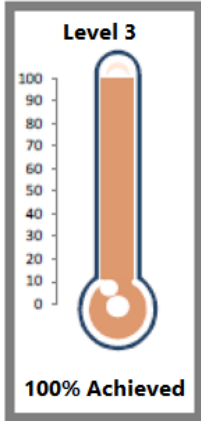
Considering the four levels of evaluation that were defined before the tests were performed, the following results were obtained:



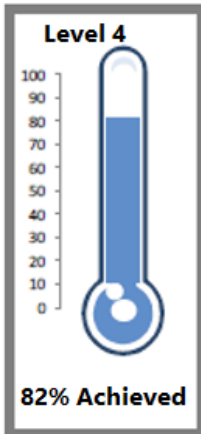
For the first evaluation level (Activation), the countries were able to share their keys (signatures), and to upload and download the keys for other countries in 100% of the tests that were performed.



For the second evaluation level, Issuance, the tests considered the standards set forth by EU-DCC. All countries were able to issue certificates in 100% of the tests that were performed.























For the third evaluation level, Verification, the certificates which were generated and uploaded into the corresponding platform were valid certificates in 100% of the tests that were performed



For the fourth evaluation level, Validation, the validation had to be carried out in a predefined timeframe. Once that timeframe had passed, it did not allow for any validations to be performed. The current test allowed for the Validation of 82% of the tests that were performed.

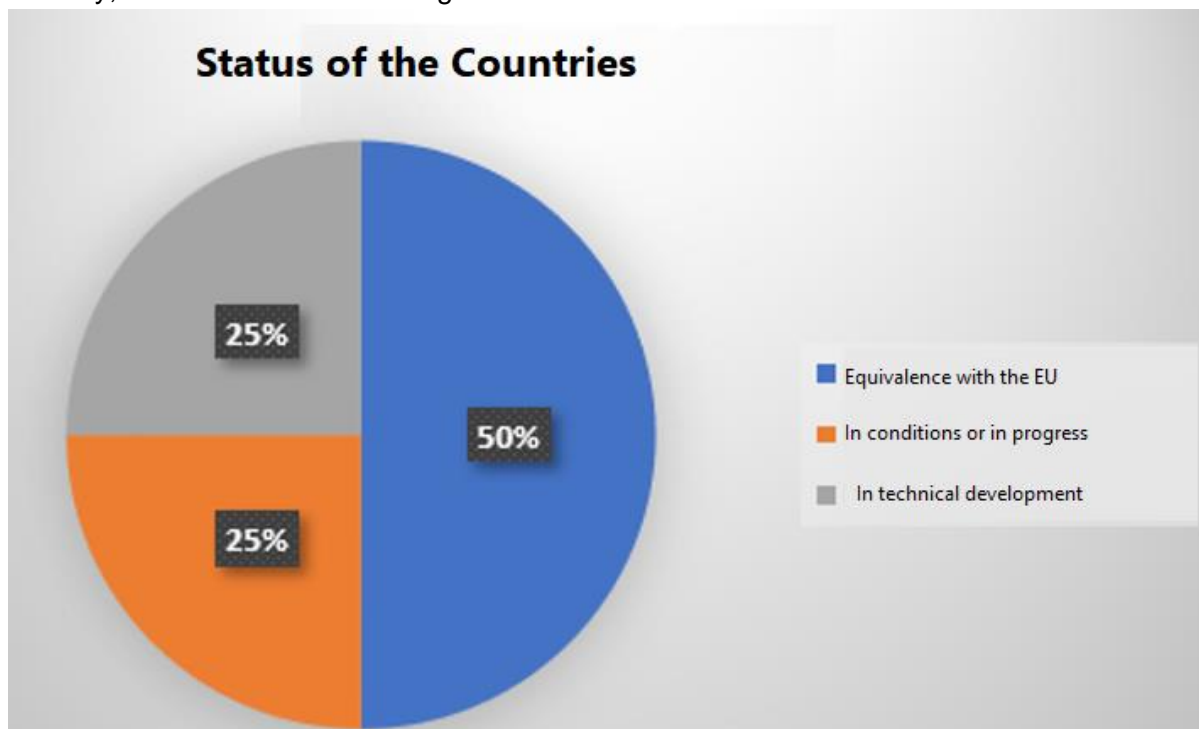
Once the Conectaton LACPASS tests were completed, we were able to determine the status of the participating countries as compared with the EU equivalent:

COUNTRY	Centralized Repository	JSON Schema	EU Subsets	CBOR/ COSE	SIGNATURE	Validator	UE Equivalent
	Yes	Equivalent	To be developed	-----	PKI	-----	
	Yes	Equivalent	Equivalent	Equivalent	CV/PKI	OK	
	Yes	Equivalent	Proprietary Codes	In Test environment	PKI (test)	In Test environment	
	Yes	Equivalent	Proprietary Codes	Equivalent	In Development	In Development	
	Yes	Equivalent	Equivalent	Equivalent	PKI	OK	
	Yes	Equivalent	Equivalent	Equivalent	PKI	OK	
	Yes	Equivalent		Equivalent	PKI	OK	
	In Development	In Test environment	In Test environment	In Test environment	PKI	In Test environment	
	Yes	Equivalent	Equivalent	Equivalent	PKI	OK	

 Equivalente con UE en Producción  
 En condiciones o en proceso de Onboarding con UE  
 En Desarrollo Técnico

We found that there were four countries that currently have an equivalence with the EU, two which are undergoing technical developments, and two in the process or conditions to validate the equivalence. It is important to note that Argentina did not participate in the event.

Visually, the status is the following:



## Conectaton LACPASS Survey

After the event was completed, the Conectaton LACPASS organization decided to carry out a Survey between the participating countries to learn more about their opinion regarding the whole process until the Conectaton was carried out.

The survey had three blocks: the first block was aimed at learning about the status of the country for COVID-19 certificates considering that the goal was to get to the same state the European Union has for COVID-19 certificates.

The second block included questions related to the event, whether there were any difficulties in any of the levels, to gather their opinion regarding the talks provided during the Conectaton LACPASS, and the materials that were provided with technical information.

For the third block, we wanted to know more about any improvements that could be introduced for future events with similar characteristics in order to strengthen the quality of these types of events at a Regional level. Lastly, we asked respondents to include a final statement which would be enriched with other events carried out in Latin America and the Caribbean.

The following is an analysis of the responses obtained from the Survey. The survey was answered by 8 countries: Chile, Colombia, Ecuador, El Salvador, Paraguay, Peru, Suriname and Uruguay.

In relation to Digital COVID Certificates, the situation between the countries varies according to the existing certificates. For COVID-19 vaccination certificates, we found that the digitization progress was different states for all countries. Three countries had been approved by the EU; the rest of the countries had digital Vaccination Certificates with QR codes and advanced digital signatures.

For Recovery Certificates, the situation is different for all countries. Only one country has a Certificate approved by the EU. All other countries do not have the Certificate; if they do have a digital version of it, it is only used by healthcare providers and not available to the general population.

Finally, for Digital Test Results Certificates, we found that only one country had a Certificate approved by the EU. Among the other countries, only two have digital certificates available to the general population through applications local to each country.

After the survey, we tried to learn more not only about the perception that they had before the event, but also about their opinion regarding the materials, talks, and technical information provided before the LACPASS Conectaton was held.

Regarding their perception before the event, all participating countries agreed about the importance of learning about the experience and the situation of the different countries in relation to their Digital Certificates.

In addition, they were able to perform different connectivity tests with other countries, which allowed them to learn as a group, because many countries had no knowledge about the tests and the situation of other countries.

Most countries had no difficulties before the event was held. However, the countries that did face some difficulties mentioned the following items:

- Problems when uploading the public keys using the Gateway service. The problem was solved successfully.
- Problems establishing a connection to the Gateway. The problem was solved successfully.
- Problems related to the trip and travel expenses, related to their country, unrelated to the event.

When we asked the participating countries for their opinion regarding the talks, the Webinar, and technical materials provided by the organization, all of them agreed that the provided materials were very complete and were high-quality. They provided them with the information that they needed to perform the requested tests.

Regarding their opinion on the talks that were provided, we specifically asked about the information regarding the IPS profile (International Patient Summary) where, again, all countries agreed that the information provided regarding the IPS was high-quality. Each country highlighted that they were able to learn more about the IPS to work on it further.

For the second block of questions, we were interested in learning about the participants' opinions regarding the event itself. The first thing we wanted to learn more about was whether or not they had had any issues, and, if they had, what those issues had been.

With regards to this point, the participants mentioned that they only had connectivity issues due to the Wifi during the first day of the event, but these were solved quickly and successfully, which allowed for the event to carry on without any further hindrances.

To learn more about the testing process, we asked participants if they had any problems at any of the levels. We received the following responses:

- Level 1- Activation: no countries reported having had any issues at this level.
- Level 2- Issuance: no countries reported having had any issues at this level.
- Level 3- Verification: there were some issues at this level. Two countries reported having issues when verifying the QR codes, specifically for Uruguay.
- Level 4- as mentioned before, two countries reported having issues when Validating the QR codes for Uruguay. This issue was related to the use of DGCA-App-Core-

Android-Main, which made it difficult to Validate QR codes for Uruguay. The cause of this was that the public keys for Uruguay were not present in the Verifier's signercertificateStatus, so the QR codes for Uruguay could not be validated.

Once the test concluded, the participants were asked how they would evaluate the synergy achieved between all countries participating in the Conectaton LACPASS. Generally, all countries evaluated the generated synergy as excellent, but they also noted that no specific exchange instances were generated between the countries because each delegation was focused on their own tests.

Similarly to the start of the survey, we also asked what the situation was regarding COVID-19 Digital Certificates for each of the participating countries. It was also very interesting for us to learn each country's stance regarding the implementation of these Certificates.

We found very varied opinions regarding the certificates, as detailed below:

- Vaccination Certificates: we found that three countries have certificates approved by the EU, the rest of the countries are currently developing the Certificates or are implementing them. They also meet the steps required to receive the approval from the EU.
- COVID-19 Recovery Certificates: only one country has certificates approved by the EU. Five countries have no Recovery digital certificates, and the rest of the countries have certificates, but they are only used by the healthcare providers.
- COVID-19 Test Results Certificates: only one country issues certificates approved by the EU. There are three countries with digital COVID-19 test result certificates. The others do not have the certificate.

We also asked the participating countries whether they were planning to implement the guidelines proposed by RACSEL in production, or whether they thought any guidelines could not be carried out. In this case, all countries agreed that their intention was to implement the guidelines provided by RACSEL. Only one country has started the work to implement the IPS.

Because Conectaton LACPASS was the first event held in Latin America and the Caribbean, the participants were asked to provide improvement suggestions for future similar events to be carried out. We found that 55.5% of the countries (5) had no improvement suggestions for future events, with 45.5% (4) including the following improvements:

- Improving the WIFI connection.
- Having more clear information related to travelling, travelling expenses, and stays.
- Having technical adjustments done before the QR Validation activity. This was related to some countries not being able to read the QR codes for Uruguay.

- In future events, including a case with digital certificates such as registering for the event. This way, the participants can use the technology.

At the end of the survey, we asked participants to share a final comment regarding the whole Conectaton LACPASS process to meet the goal we had set out regarding the testing process. The comments were as shared below:

- There are many things that have already been resolved technically speaking, it's just a matter of wanting to do it.
- The event was very rewarding, the experience of sharing achievements, lessons learned, and actions to transform Digital Health in our countries, to share challenges and learn from mistakes made in the region so we don't make those same mistakes, in addition to the good experiences to be able to implement them. It is through these events that we create a community where ideas can be presented and support provided when needed from another country. Seeing the breakthroughs in the region motivates us to work even harder so we don't fall behind in the Digital Transformation process.
- The organization and testing modality overlapping with other countries was very friendly and easy to use.
- It has been very rewarding work to learn about the technology used by the EU and to implement something like that in our national systems.
- The management and preliminary meetings before Conectaton were crucial for the success of the tests; for this preparation, management, and coordination Congratulations. The only thing I would recommend for future instances is having a backup Internet channel to avoid the issue we had the first day of the Conectaton.
- To have more consecutive events such as this one to have more speedy implementations together with other countries, technology that allows us to have the International Electronic Clinical History.
- It was a very organized process with a lot of preparation given that the management of the event had been happening since December.
- It was a great learning experience, knowing what our neighboring countries are up to and what we are looking at for the future.
- When performing the tests, it was very helpful to have technical personnel who offered their assistance during the whole event.
- These initiatives in Latin America foster Interoperability in the Healthcare Industry and are motivating to work to help the population, the participation of international organisms and the IADB financing is very important, it is a very good opportunity to network and share experiences regarding success stories and misses for each country, I am really very grateful for the opportunity of participating in the CONECTATON LACPASS.
- The most important goals were met because the certificates could be validated for other countries in the region.

Generally, all participating countries highlighted the good quality of the technical material that was provided during each of the event's instances, in addition to the talks. This was a crucial aspect to them because the good quality of the information allowed for all participants to be motivated in becoming interested in all topics that were raised.

## Future steps

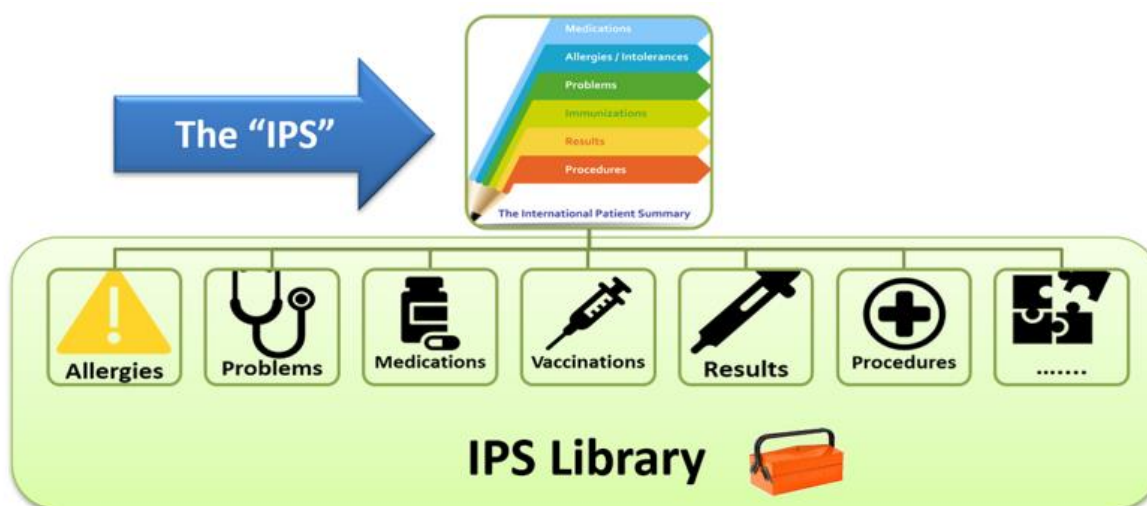
It is important to point out that the results obtained during the Conectaton event were favorable. We were able to meet all the interoperability goals that were defined for all participating countries.

In addition, we have been able to move forward to component 02 of the Regional Public Goods, starting with new trainings related to the progress towards the new component. These trainings are:

- Gazelle training.
- IPS Profile.
- MDH Profile.

This has enabled new interoperability instances between the countries which allows for them to focus on moving forward to the inclusion of IPS in the region.

The IPS is the International Patient Summary, a non-exhaustive system of clinical data, which makes it possible to offer personalized attention in case of an emergency. This can be brought with the patient, and it covers all privacy and security aspects.



The components are the following ones:



The intended scope for the IPS is to:

- Generate knowledge regarding the IPS.
- Generate knowledge regarding the FHIR.
- Learn more about the evolution towards the DDCC proposed by the WHO.
- Preparing use cases associated with cross-border interoperability.
- Testing FHIR and IPS resources.

## Conectaton Conclusions

After the Conectaton was completed, and the results from the tests carried out by the participating countries were obtained, we can assert that the goals we established for at least three countries to successfully complete Conectaton were met. In the case of El Salvador, they were not able to meet the validation goals because they had delays with their deadlines. After the date passed, it was not possible to validate the test.

It should be noted that all participating countries have Digital Certificates for COVID-19 Vaccinations with different degrees of evolution. Some of them have even been approved by the European Union. However, this is not the case with the COVID-19 Recovery certificate and the COVID-19 Test Results certificate.

In addition, we can also affirm that all participating countries are in position to obtain the technical equivalence necessary to obtain the European Union's certification, and, therefore, move forward with new interoperability features within the region by including the IPS.

## Lessons Learned

Conectaton LACPASS was the first event in Latin America and the Caribbean which had the goal to perform information exchange tests between participating countries. It generated a precedent and a starting point to continue a partnership between all of the countries in the region so that, in the future, they can exchange clinical information across borders, and also include the IPS.

The following is a description of the lessons we learned during Conectaton LACPASS:

- The creation of a collaborative environment to exchange information and experiences allowed the participating countries to acquire knowledge from each other's experiences and to answer any of their doubts.
- The importance of providing participants with high-quality technical information before the Conectaton LACPASS was held, which contributed towards all participants having clear information, thus creating a solid knowledge base.
- The implementation of prior preparation courses, such as talks with experts for topics related to Conectaton, such as IHE and IPS, among others.
- It is very important for this kind of event, the goal of which is to execute tests to exchange clinical information, to have a high degree of connectivity allowing for the activities to be carried out without any hindrances.
- Having a technical support team present during the whole development of the event, because it not only allows for unexpected incidents to be resolved, but it also allows for them to help participants reach the proposed goals.

# Annexes

## Annex 1- LACPASS Technical Documentation

### Introduction

This document is presented as technical documentation for the implementation of LACPASS, detailing how the solution operates and the necessary steps that participating countries must take to join LACPASS.

The Latin American and Caribbean Vaccination Pass, LACPASS, is an application for the exchange of information on vaccination status of Latin American and Caribbean countries, which allows people who have received part or all of the COVID vaccination scheme in their country of residence, when traveling to another country in the region, they can simply and verifiably validate their vaccination status in the country of destination, without the need to carry out additional procedures such as homologation of the local vaccination certificate.

The LACPASS project is an initiative of the American Network for Cooperation in Electronic Health in Latin America and the Caribbean (RACSEL), sponsored by the Inter-American Development Bank (IDB) and executed by the National Center for Information Systems of Chile (CENS) by through the private company Create de Chile, which was awarded the tender for the development and implementation of this public good.

The technology behind LACPASS is based on the Digital Green Certificates of the European Union (EU-DGC), this repository is an open source project used in all the countries of the European Union and 24 countries outside it. This pass is multilanguage and is available in English, Spanish, French and Portuguese which are of special interest in this region. In addition, it can be digital and on paper, and has a verifiable QR code through the applications provided by the DGC. By connecting interested countries to LACPASS it is possible to use the same technology to connect to the Digital Green Certificates of the European Union.

The main objective of the LACPASS project is to connect in a secure and verifiable way the information on individual vaccination of the residents of the countries of the region in a uniform and interoperable system that facilitates travel within the region by delivering to the health and immigration authorities of the countries a tool that provides accurate and timely information on the vaccination status of passengers who are entering or passing through.

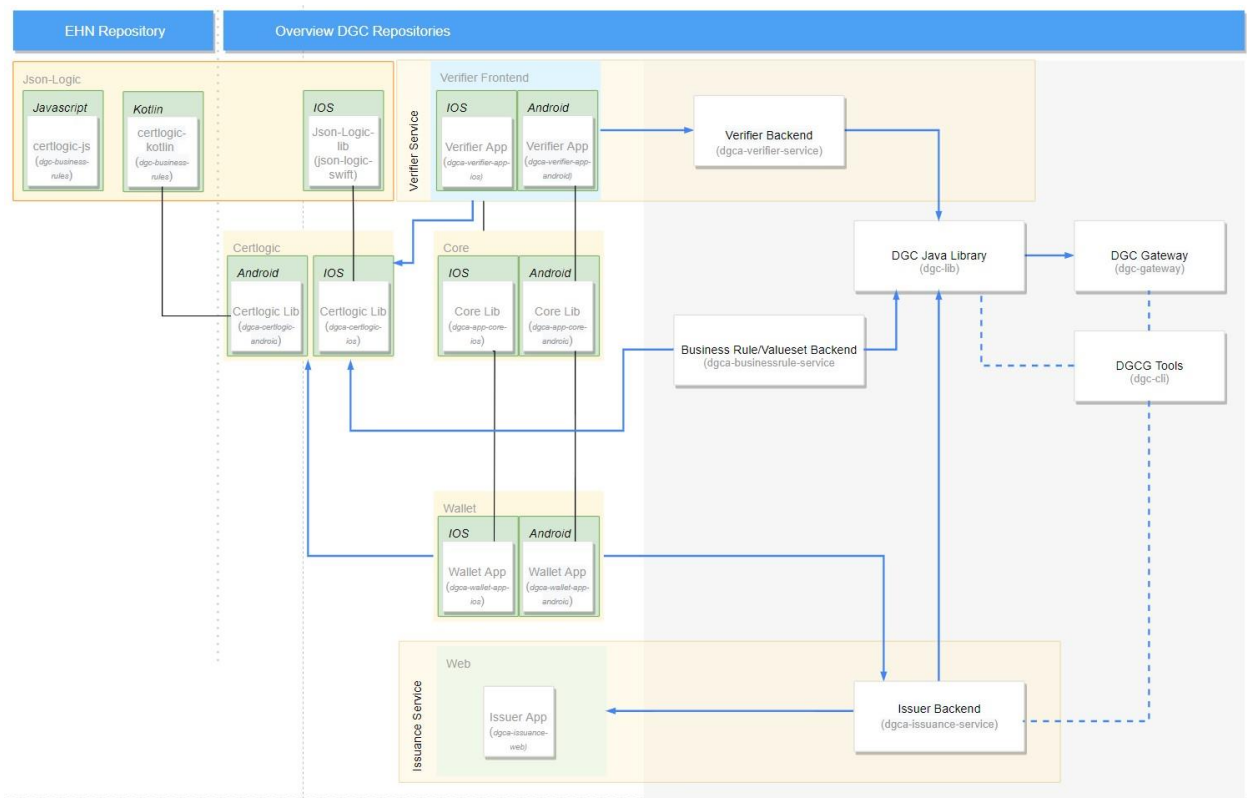
As an additional objective, it seeks to collaborate with the countries of the region so that they can connect in a simple and fluid way to the Digital Green Certificates technology of the European Union.

## Architecture

As explained above, the implementation of LACPASS is based on the Digital Green Certificates projects of the European Union (DGC) and European Health Network (EHN), whose repositories can be found at the following links:

- DGC: <https://github.com/eu-digital-green-certificates>
- EHN: <https://github.com/ehn-dcc-development>

The DGC provides different repositories for the implementation of interoperability of vaccination certificates. The interaction of all these repositories is shown in the following diagram:



Functionally the repositories can be divided into 3 groups:

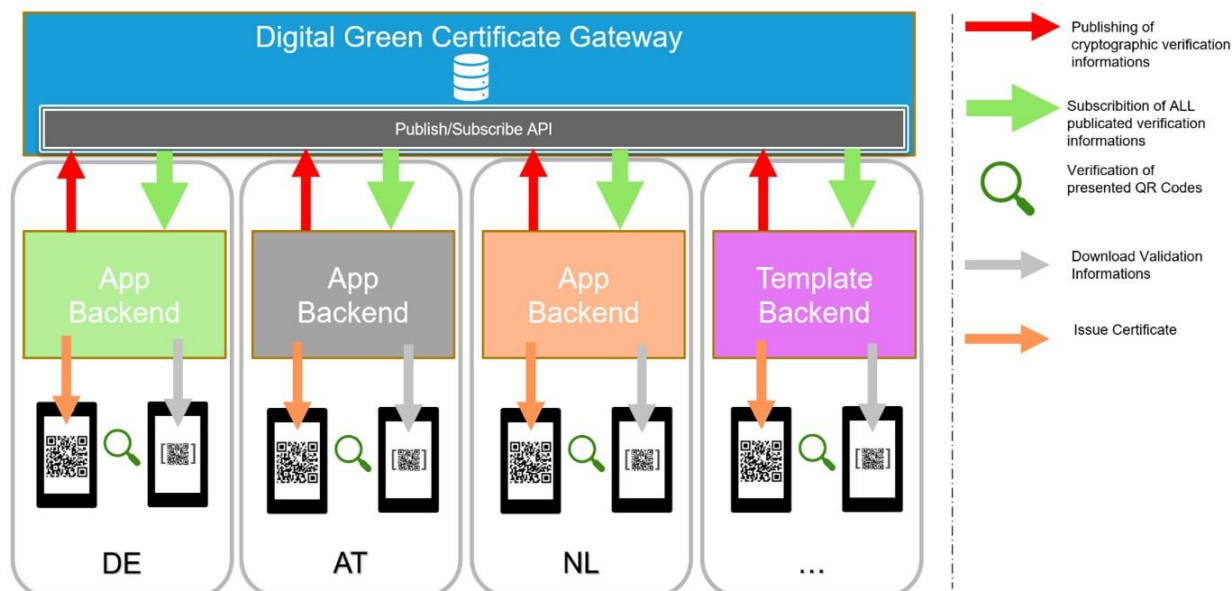
### Logic and Synchronization

## Gateway

The DGC Gateway has the purpose of serving as support for the entire DGC system, it provides all the services necessary for the secure transfer of validations and verifications between national systems. Each national system can implement its own DGC Gateway to obtain the freedom to distribute the keys with the preferred technology and also to be able to manage national verification systems.

Additionally, if the certificate is generated in a correct standard format, any verifying device will be able to verify codes of any country that has the EU format. This works for both the verifier connected to the national system and offline systems that have the necessary public keys downloaded beforehand.

The following diagram shows the flow between the different national systems and the DGC Gateway:



Here is a link to detailed documentation of the DGC Gateway ([Documentation](#)).

## Business Rule Service

The DGC Business Rule Service is one of the services connected to the DGC Gateway, this service provides the necessary rules to verify whether or not a code is valid in a national system. These rules are based on the vaccines you have, the tests performed and the recovery status of the validated person..

To generate these validation rules there is a more detailed format in this link ([Business Rules Test Data](#)).

### **Issuance**

#### **Issuance Service**

The DGC Issuance Service is the backend system that provides both the creation and signing of new certificates (green certificates). Each country must raise this service to be able to have the certificates. In order for the certificates to be used internationally, the public keys must be shared in the Gateway so that all countries can verify the certificates. This service is used by mobile applications (Android, iOS) and by web applications.

#### **Issuance Web**

The Issuance Web is a web application that provides a user interface used to provide the necessary data in the issuance service. Certificates can also be generated in this application.

### **Verification**

#### **Verifier Service**

To verify the certificates it is necessary to have the public keys of the appropriate national system. The DGC Verifier Service is a backend service that is used to manage the public keys obtained through the DGCG. This service is used in mobile applications to obtain public keys and verify green certificates.

To verify the certificates you can use both the verifier on [iOS](#) and [Android](#). Both repositories contain a very simple application to scan QR codes and a verification and validation interface for these.

## Security and Encryption Keys

The DGC system uses a security system based on the paradigm of public and private keys that are used to verify the authenticity of the queries and the signing of the certificates. Something important to note is that these public keys are verified directly by the DGC application and do not necessarily follow the usual HTTPS rules.

Within the repositories, different formats and standards are used for saving keys, each of these formats is described below:

- **PEM:** File containing a public key and optionally a private key in flat form. Usually only the public key is included.

- **KEY:** File containing a private key in a flat shape. This file **should never be shared** with third parties to avoid attacks and vulnerabilities.
- **P12:** File that contains a public key and optionally a private one, encrypted by a password. Normally a PEM file is taken as input to build a P12.
- **JKS:** Format similar to P12 that is able to be read by Java applications in a simple way.

## Implementation

This section describes the steps that need to be taken for a new participating country to be included in LACPASS.

### Technologies

The “*EU Digital Covid Certificates*” (EUDCC) repositories provide APIs that are developed in the Spring Framework using Java as the primary programming language. The databases used are Mysql and Postgresql. The certificate issuance web application is developed in React. And the mobile apps are natively developed on Kotlin (Android) and Swift (iOS). All projects except mobile apps are available through Docker.

### Server Requirements

A server is required which will host the web services repositories. The characteristics of this server will depend on the estimated traffic, but a server with at least 4 vCPUs, 8 Gb of RAM and 50 Gb of disk is recommended.

A server is required which will host the web services repositories. The characteristics of this server will depend on the estimated traffic, but a server with at least 4 vCPUs, 8 Gb of RAM and 50 Gb of disk is recommended.

### Pre-requirements

The steps to follow to create each of the EUDCC repositories will be given below. Pre requirements:

- OpenJDK 11
- Maven
- Authenticate with [Github Packages](#)
- Docker (optional)
- Docker-compsoe (optional)
- Node 14
- OpenSSL
- [DGC-CLI](#)

In order to install the dependencies through Maven in the repositories that use Spring as technology, you need to be authenticated by Github. For this you need to create a [personal access token](#), which has the option "read: packages" selected. Then you must fill in the maven configuration file (in linux located in ~/.m2/settings.xml) like the one shown below:

```
<?xml version="1.0" encoding="UTF-8"?>
<settings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://maven.apache.org/SETTINGS/1.0.0"
xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.0.0
https://maven.apache.org/xsd/settings-1.0.0.xsd">
  <interactiveMode>false</interactiveMode>
  <servers>
    <server>
      <id>dgc-github</id>
      <username>$USER</username>
      <password>$TOKEN</password>
    </server>
    <server>
      <id>ehd-github</id>
      <username>$USER</username>
      <password>$TOKEN</password>
    </server>
  </servers>
</settings>
```

## Gateway

The gateway is used to share and verify information through all the countries connected to it. Therefore, it should not be included in the backend of each country, here it is explained how to set up a gateway only in order to be able to test the connection of other services. The repository can be cloned using:

```
$ git clone https://github.com/eu-digital-green-certificates/dgc-gateway
```

## Keys

To run it locally you need to create a TrustAnchor. The TrustAnchor is used to sign entries in the database. To create the TrustAnchor the following command is used:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key_ta.pem -out cert_ta.pem
-days 365 -nodes
```

Then the public key is exported to the Java Keystore using:

```
$ keytool -importcert -alias dgcg_trust_anchor -file cert_ta.pem -  
keystore ta.jks -storepass dgcg-p4ssw0rd
```

Where "cert\_ta.pem" is the public key and "dgcg-p4ssw0rd" is the password of the public key. This "ta.jks" key must be placed in a folder named "certs", which must be created in the root of the repository.

### Database

This repository uses a MySQL database, if docker is not used to build the project, you need to install and create a base in MySQL.

### Configuration

To configure variables such as the directory of the public key and the connection to the database, it can be done in two ways. If Docker is used to run the project, the environment variables shown in "docker-compose.yml" can be edited. For more details on this file, the documentation is available at the following link. If docker is not used, you can edit the Spring configuration file in "~/dgc-gateway/src/main/resources/application.yml"

### Execute

To build the project executable, through Maven, use the following command:

```
$ mvn clean install
```

If docker is used to run the project, an extra flag must be added to the previous command:

```
$ mvn clean install -P docker
```

This will create a "jar" file in the "~/dgc-gateway/target" directory. To run the application you use:

```
$ java -jar target/dgc-gateway-latest.jar
```

And if you use Docker, you can use:

```
$ docker-compose up --build
```

Which will upload the gateway API along with a mysql database. In order to query the API of this gateway, it is necessary to register certain certificates that belong to the backend of each country. These certificates will be from AUTHENTICATION, UPLOAD and CSCA. For this, these certificates can be created with OpenSSL:

```
# AUTHENTICATION
```

```

$ openssl req -x509 -newkey rsa:4096 -keyout key_auth.pem -out
cert_auth.pem -days 365 -nodes

# CSCA
$ openssl req -x509 -newkey rsa:4096 -keyout key_csca.pem -out
cert_csca.pem -days 365 -nodes

# UPLOAD
$ openssl req -x509 -newkey rsa:4096 -keyout key_upload.pem -out
cert_upload.pem -days 365 -nodes

```

These certificates must be signed by the TrustAnchor of the gateway ("cert\_ta.pem" and "key\_ta.pem"), for this the client provided by the EUDCC can be used. This can be downloaded at this link. Then using this jar, the following commands can be executed:

```

$ java -jar dgc-cli.jar ta sign -c cert_ta.pem -k key_ta.pem -i
cert_auth.pem
$ java -jar dgc-cli.jar ta sign -c cert_ta.pem -k key_ta.pem -i
cert_csca.pem
$ java -jar dgc-cli.jar ta sign -c cert_ta.pem -k key_ta.pem -i
cert_upload.pem

```

In each of these commands a "TrustAnchor Signature", "Certificate Raw Data", "Certificate Thumbprint" and "Certificate Country" will be delivered. These values have to be entered in the "trusted\_party" table of the gateway database, so three new lines will be added in this table (for each of the certificates). This can be done using:

```

$ mysql --user=root --password=admin dgc
$ INSERT INTO trusted_party (created_at, country, thumbprint, raw_data, signature,
certificate_type)
SELECT
    NOW() as created_at,
    'CL' as country,
    '{Certificate_Thumbprint}' as thumbprint,
    '{Certificate_Raw_Data}' as raw_data,
    '{TrustAnchor_Signature}' as signature,
    '{AUTHENTICATION|UPLOAD|CSCA}' as certificate_type;

```

To test that the values were entered correctly, a request can be made to the gateway API using the authentication thumbprint:

```
$ curl -X GET http://localhost:8080/trustList -H "accept: application/json" -H "X-SSL-Client-SHA256: $THUMBPRINT" -H "X-SSL-Client-DN: C=$COUNTRY"
```

Which should deliver the list of certificates in the table "trusted\_parties".

## Business rule

This repository contains a backend with the business rules to accept / reject the states of the COVID certificates issued by the countries. The repository can be cloned using:

```
$ git clone https://github.com/eu-digital-green-certificates/dgca-businessrule-service
```

## Keys

This repository requires three keys, a trust\_anchor, trust\_store, and key\_store. The trust\_anchor is the TrustAnchor created in the gateway, the trust\_store can be created using the certificate and authentication key that were registered in the gateway as follows:

```
$ openssl pkcs12 -export -in cert_auth.pem -inkey key_auth.pem -name 1 -out tls_key_store.p12
```

The truststore is created using the authentication certificate, with the command:

```
$ openssl pkcs12 -export -in cert_auth.pem -name tls_trust -out tls_trust_store.p12 -nokeys
```

## Database

This repository uses a Postgresql database, if docker is not used to build the project, you need to install and create a Postgresql database.

## Configurations

To configure variables such as the directory of the keys and the connection to the database, it can be done in two ways. If Docker is used to run the project, the environment variables shown in "docker-compose.yml" can be edited. For more details on this file, the documentation is available at the following link. If docker is not used, you can edit the Spring configuration file in "~/dgc-gateway/src/main/resources/application.yml". The most important variables are shown below:

```
# Credenciales base de datos
SPRING_DATASOURCE_URL=<CONNECTION_URL>
SPRING_DATASOURCE_USERNAME=<USER>
SPRING_DATASOURCE_PASSWORD=<PASSWORD>
# Gateway endpoint
DGC_GATEWAY_CONNECTOR_ENDPOINT=https://test-dgcg-ws.tech.ec.europa.eu
```

```
# Certificados
DGC_GATEWAY_CONNECTOR_TLSTRUSTSTORE_PATH=<PATH>
DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_ALIAS=<ALIAS>
DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PATH=<PATH>
DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PASSWORD=<PASSWORD>
DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_ALIAS=<ALIAS>
DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PATH=<PATH>
DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PASSWORD=<PASSWORD>
```

## Run

To build the project executable, which is built through Maven, the following command is used:

```
$ mvn clean install
```

This will create a "jar" file in the "~/dgc-businessrule-service/target" directory. To run the application you use:

```
$ java -jar target/dgc-businessrule-service-latest.jar
```

And if you use Docker, you can use:

```
$ docker-compose up --build
```

## Rules

This section briefly explains how to generate a JSON file with the certificate validation rules. These rules determine if a person who enters a country is considered suitable to enter this country, the rules are based on the vaccines administered, the tests they have performed and the state of recovery after contracting COVID. All these rules must be encoded according to the standards of the Digital COVID Certificate.

To generate the validation rules it is required to generate a json with the following:

- Valid as a [CertLogic](#) expression.
- The JSON file of every rule is validated against this [JSON Schema](#).
- The specified AffectedFields field is checked against the fields of the DCC payload accessed from the Logic field. ([DCC Schema](#))

CertLogic is a semantics subset that extends the [JsonLogic](#) semantics. These semantics use intuitive and simple rules to be able to verify patterns or logic within a Json file. They use logical operators such as equality ("=="), numeric operators, and so on. These operators can be found [here](#).

Here is an example of how a Json is constructed with the CertLogic semantics:

```
{
  "<operation id>": [
    <operand 1>,
    <operand 2>,
    // ...
    <operand n>
  ]
}
```

Now to generate a file with the correct [standards](#), the scheme must be followed correctly, for this the following fields must be added:

- **AffectedFields:** Arrangement of rules to be used from the payload (QR).
- **Country:** ISO country code. (e.g. "CL").
- **CertificateType:** Certificate type. Valid values are "General", "Test", "Vaccination", "Recovery". If, for example, the rule looks for the minimum time after a COVID test, this certificate is of the "Recovery" type.
- **Description:** Fix with the description of the rule, here all the languages that you want to support are added.
- **Engine:** Type of semantics used. (e.g. "CERTLOGIC")
- **EngineVersion:** Version of the semantics. Currently "1.2.2".
- **Identifier:** Unique identifier for the rule. It must be the pattern `^(GR|VR|TR|RR|IR)-[A-Z]{2}-\d{4}$`. For example, if the rule is "Recovery", the country is Chile and it is also the first rule, the identifier is "RR-CL-0000".
- **Logic:** Object where the rule is established. Here semantics are used to define the rule.
- **SchemaVersion:** Version of the schema used.

- **Type:** Type of the rule, it can be of acceptance (“Acceptance”) or invalidation (“Invalidation”).
- **ValidFrom:** Until what date this rule is valid (without ms and with time zone).
- **ValidTo:** From what date this rule is valid (without ms and with time zone).
- **Version:** Rule version.

To better understand how this file is generated, it will be explained in a general way how to construct the “Logic” and “AffectedFields” fields. For the field "AffectedFields" it must be understood how the payload arrives (content of the QR), the content has a standard format that can be found at this [link](#). The payload object must contain at least one of the following fields:

- “v”: Contains everything related to vaccination (“Vaccination Entry”).
- “t”: Contains everything related to the tests performed (“Test Entry”).
- “r”: Contains everything related to recovery (“Recovery Entry”).

Each of these fields can contain specific attributes to what it represents, we will detail in the following points what each one can contain.

### **Vaccination Entry (“v”)**

- tg: Disease or target agent.
- vp: Vaccine or prophylaxis.
- mp: Vaccine drug.
- ma: Authorized marketing company or manufacturer.
- dn: Dose Number.
- sd: Total doses (Series of doses, for example would be 2 if two doses are required).
- dt: Vaccination date.
- co: Country of vaccination.
- is: Certificate issuer.
- ci: Unique identifier of the certificate (UVCI).

### **Test Entry (“t”)**

- tg: Disease or target agent.
- tt: Type of test.
- nm: Nucleic acid test.
- ma: Rapid antigen test name and manufacturer.
- sc: Date/Time of sample collection.
- tr: Test result..
- tc: Center in charge of the examination.
- co: Test country.

- is: Certificate issuer.
- ci: Unique identifier of the certificate (UVCI).

### **Recovery Entry (“r”)**

- tg: Disease or target agent.
- fr: Nucleic acid test first positive date.
- co: Test Country..
- is: Certificate issuer.
- df: Date from which the exam is valid.
- du: Date until when the exam is valid.
- ci: Unique identifier of the certificate (UVCI).

There is an official document on the documentation of this standard, in this [link](#).

To better understand how the values are chosen, we will take as an example the rule "Vaccination series must be complete (eg 1/1, 2/2)". For this example the values of "AffectedFields" would be the following:

```
"AffectedFields": [
  "v.0", // Vaccination values are required.
  "v.0.dn", // Current dose.
  "v.0.sd" // Total number of doses in the series.
]
```

Now understanding how the "AffectedFields" is assembled, following the same example, we are going to build the logic of the rule: "The vaccination schedule must be complete (for example, 1/1, 2/2)". The first thing to note is that it is a vaccination rule so the "v" part of the payload is used. In addition, as it seeks to verify the vaccination series, both "dn" and "sd" will be used where we will obtain the information of the current dose and the total of doses required respectively. Then, to validate the complete vaccination scheme, it must be verified that both values are the same, as shown in the following scheme:

```

"Logic": {
  "if": [ // If the content is met, the rule is accepted.
    {
      "var": "payload.v.0" // Where to obtain the values is made explicit.
    },
    {
      "===": [ // The exact equality operator is used.
        {
          "var": "payload.v.0.dn" // Current Dose (Number in the series).
        },
        {
          "var": "payload.v.0.sd" // Total number of doses in the series.
        }
      ]
    }
  ]
}

```

This example was taken from the rules of Spain [here](#). If you need more examples you can see those recommended by the EU ([More examples](#)).

## Issuance

This repository contains a backend that allows the issuance of vaccination certificates. The repository can be cloned using the following command:

```

$ git clone
https://github.com/eu-digital-green-certificates/dgca-issuance-service

```

## Keys

This project does not require creating new keys, the same ones previously created for the business rule will be used. In fact, instead of copying the keys between the repositories, it is recommended to have a directory where all the repositories share the keys and are shared through symbolic links or docker volumes.

## Database

This repository uses a Postgresql database, if docker is not used to build the project, you need to install and create a Postgresql database.

## Configurations

Like the business rule, the repository configuration is in the docker-compose.yml file, but you can also change the "src/main/resources/application.yml" file directly if you don't use docker.

The issuance service has two forms of execution: one for testing and the other connected to a gateway. Both are explained below:

**Testing Configuration:** This is the one that comes by default and is used to quickly test the issuance of certificates without having to install a gateway. No further configuration is required to operate in this mode and a generic test key is used to sign the certificates.

**Production Configuration:** This configuration connects to a gateway and allows interoperation with the other DGC services. To access this configuration you have to change the `docker-compose.yml` and add the following configurations to the backend

```
backend:
  environment:
    ... # KEEP WHAT IS AND ADD THE FOLLOWING
    # EMISION DE CERTIFICADOS
    - ISSUANCE_DGCIPREFIX=URN:UVCI:V1:CL
```

```

- ISSUANCE_KEYSTOREFILE=/app/certs/CL/firmasalud.jks
- ISSUANCE_KEYSTOREPASSWORD=dgcg-p4ssw0rd
- ISSUANCE_CERTALIAS=firmador
- ISSUANCE_PRIVATEKEYPASSWORD=dgcg-p4ssw0rd
- ISSUANCE_COUNTRYCODE=CL
- ISSUANCE_EXPIRATION_VACCINATION=365
- ISSUANCE_EXPIRATION_RECOVERY=365
- ISSUANCE_EXPIRATION_TEST=60
# SERVICIOS DISPONIBLES
- ISSUANCE_ENDPOINTS_FRONTENDISSUING=true
- ISSUANCE_ENDPOINTS_BACKENDISSUING=true
- ISSUANCE_ENDPOINTS_TESTTOOLS=true
- ISSUANCE_ENDPOINTS_WALLET=true
- ISSUANCE_ENDPOINTS_PUBLISHCERT=true
- ISSUANCE_ENDPOINTS_DID=true
# CONFIGURACION DE GATEWAY
- DGC_GATEWAY_CONNECTOR_ENABLED=true
- DGC_GATEWAY_CONNECTOR_ENDPOINT=https://lacpass.example.com:3050
- DGC_GATEWAY_CONNECTOR_PROXY_ENABLED=false
- DGC_GATEWAY_CONNECTOR_PROXY_HOST=
- DGC_GATEWAY_CONNECTOR_PROXY_PORT=-1 - DGC_GATEWAY_CONNECTOR_MAX-
  CACHE-AGE=300 -
DGC_GATEWAY_CONNECTOR_TLSTRUSTSTORE_PATH=file:/app/certs/tls_trust_store
.p12
- DGC_GATEWAY_CONNECTOR_TLSTRUSTSTORE_PASSWORD=dgcg-p4ssw0rd-
DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PATH=file:/app/certs/tls_key_store.p12
- DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PASSWORD=dgcg-p4ssw0rd
- DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_ALIAS=tls_key
- DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PATH=file:/app/certs/ta.jks
- DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PASSWORD=dgcg-p4ssw0rd
- DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_ALIAS=trustanchor-
DGC_GATEWAY_CONNECTOR_UPLOADKEYSTORE_PATH=file:/app/certs/CL/upload_key_
store.p12
- DGC_GATEWAY_CONNECTOR_UPLOADKEYSTORE_ALIAS=upload_key
- DGC_GATEWAY_CONNECTOR_UPLOADKEYSTORE_PASSWORD=dgcg-p4ssw0rd

```

Make sure you replace the keys correctly. More information about this configuration in [this link](#).

## Run

To build the project executable, which is built through Maven, the following command is used:

```
$ mvn clean package
```

This will create a "jar" file in the "~/dgc-issuance-service/target" directory. To run the application you use:

```
$ java -jar target/dgc-issuance-service-latest.jar
```

And if you use Docker, you can use:

```
$ docker-compose up --build
```

At the end, the web service that issues certificates should be started on the port indicated in the configuration. For example, if port 8081 is used, you can navigate to this URL:

<http://localhost:8081/swagger>

## Web Client

To test the issuance of certificates, the DGC provides another repository called [issuance-web](#). This is a web application that consumes the API delivered by the issuance-service and allows the generation of vaccination certificates. This application works independently if Testing mode or productive mode was chosen in issuance-service. To clone the repository, you run the following command:

```
$ git clone https://github.com/eu-digital-green-certificates/dgca-issuance-web
```

Then to connect with the APIs it is necessary to modify the docker-compose.yml file, or change the nginx configuration file.

```
- DGCA_ISSUANCE_SERVICE_URL=http://dgc-issuance-service:8081
- DGCA_BUSINESSRULE_SERVICE_URL=http://dgc-businessrule-service:8082
```

Here you must specify the URLs of the issuance-service and business rule. Something important to note is that this repository brings these two services as dependencies, since in this guide we are setting up and configuring each service separately, it is necessary to remove these from the configuration.

Finally you can run the web application using the following command

```
$ docker-compose up --build
```

## Verifier

This repository contains a backend that allows the verification of vaccination certificates issued. The repository can be cloned using the following command:

```
$ git clone https://github.com/eu-digital-green-certificates/dgca-verifier-service
```

## Keys

Like the issuance service, this repository needs the previously created keys.

## Database

This repository uses a Postgresql database, if docker is not used to build the project, you need to install and create a Postgresql database.

## Configurations

Like the issuance-service, the repository configuration is in the docker-compose.yml file, but the "src/main/resources/application.yml" file can also be changed directly in case of not using docker.

There is no testing mode for the verifier-service, so it is always used with an associated gateway. To configure it, it is necessary to modify the configuration file and indicate the routes to the gateway and the keys:

```
- DGC_GATEWAY_CONNECTOR_ENDPOINT=https://dgc-gateway.example.com-
DGC_GATEWAY_CONNECTOR_TLSTRUSTSTORE_PATH=file:/ec/prod/app/san/dgc/tls_trus
t_store.p12
- DGC_GATEWAY_CONNECTOR_TLSTRUSTSTORE_PASSWORD=dgcg-p4ssw0rd
- DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_ALIAS=1 -
DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PATH=file:/ec/prod/app/san/dgc/tls_key_st
ore.p12
- DGC_GATEWAY_CONNECTOR_TLSKEYSTORE_PASSWORD=dgcg-p4ssw0rd
- DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_ALIAS=ta-
DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PATH=file:/ec/prod/app/san/dgc/trust_anch
or.jks
- DGC_GATEWAY_CONNECTOR_TRUSTANCHOR_PASSWORD=dgcg-p4ssw0rd
```

## Run

Like the previous repositories, to build the project executable, the following Maven command is used:

```
$ mvn clean install
```

This will create a "jar" file in the "~/dgc-verifier-service/target" directory. To run the application you use:

```
$ java -jar target/dgc-issuance-verifier-latest.jar
```

And if you use Docker, you can use:

```
$ docker-compose up --build
```

At the end, the web service that issues certificates should be started on the port indicated in the configuration. For example, if port 8082 is used, you can navigate to this URL:

<http://localhost:8082/swagger>

## Verification Mobile Apps

For mobile applications the repositories are divided into the iOS and Android platforms. Both platforms have 4 repositories divided by functionalities that each one fulfills. For the development of applications to verify the certificates, only the "verifier" and "wallet" repositories will be modified according to what is needed. The repositories for both platforms are as follows:

- **App Core:** This repository contains all the services necessary to connect to the DGC Verifier Service and to the DGC Business Rule. It is also responsible for signing the certificates to be able to send them safely.
  - iOS: <https://github.com/eu-digital-green-certificates/dgca-app-core-ios>
  - Android: <https://github.com/eu-digital-green-certificates/dgca-app-core-android>
- **Verifier:** This repository contains the mobile application that is in charge of scanning and verifying the certificates using the public keys, it uses the App Core to make the pertinent calls.
  - iOS: <https://github.com/eu-digital-green-certificates/dgca-verifier-app-ios>
  - Android: <https://github.com/eu-digital-green-certificates/dgca-verifier-app-android>
- **Wallet:** This repository provides a user interface to manage and save personal DGCs.
  - iOS: <https://github.com/eu-digital-green-certificates/dgca-wallet-app-ios>

- Android: <https://github.com/eu-digital-green-certificates/dgca-wallet-app-android>
- **CertLogic:** This repository contains the source code to handle CertLogic semantics in mobile applications.
  - iOS: <https://github.com/eu-digital-green-certificates/dgc-certlogic-ios>
  - Android: <https://github.com/eu-digital-green-certificates/dgc-certlogic-android>

In case QR code examples are required, there are these official examples (<https://dgc.a-sit.at/ehn/testsuite>).

## IOS

The requirements for services on iOS are:

- A Mac or virtual machine is required to run Xcode.
- Xcode 12.5+ is used for builds. A macOS 11.0+ operating system is required.
- To install it on physical devices, an Apple developer account is required. For this you must enroll in the apple development program ([Apple Developer Program](#))

## Verifier

This repository contains the mobile application to verify certificates through iOS. In order to install this project you must first clone it locally with the following command:

```
$ git clone
https://github.com/eu-digital-green-certificates/dgca-verifier-app-ios
```

In order to have the connection and certificate signing services, you must also have the core repository in the same folder, you can use the same command used to clone the core repository.

```
<project folder>
|__dgca-app-core-ios
|__dgca-verifier-app-ios
```

Once you have both repositories installed, they must modify the context.jsonc file with the correct national system values. This file is located in the “context” folder. You must fill in the appropriate values as shown in the following diagram:

```

{ // Origin in ISO alpha 2 code:
  "origin": "XX",
  "versions": {
    "default": {
      "privacyUrl": "https://<PRIVACY_URL>",

      "context": { "url":
        "https://<URL_ISSUANCE_SERVICE>/context",
        "pubKeys": [<PUBLIC_KEYS>]
      },
      "endpoints": {
        "claim": { "url":
          "https://<URL_ISSUANCE_SERVICE>/dgci/wallet/claim",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "countryList": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/countrylist",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "rules": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/rules",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "valuesets": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/valuesets",
          "pubKeys": [<PUBLIC_KEYS>]
        }
      }
    }
  },
}

```

Once you have these values, you can run the certificate validation application.

To modify the Locale of the app you just have to generate a new locale file inside the folder “Localization/DGCAVerifier”. Copy the file en.xloc and modify it to meet your localization.

### Wallet

This repository contains the mobile application to save and manage personal certificates. In order to install this project you must first clone it locally with the following command:

```

$ git clone
https://github.com/eu-digital-green-certificates/dgca-wallet-app-ios

```

In order to have the connection and certificate signing services, you must also have the core repository in the same folder, you can use the same command used to clone the core repository.

```
<project folder>
|__dgca-app-core-ios
|__dgca-wallet-app-ios
```

Like the verifier, you must modify the context.jsonc in order to generate the personal certificate. You can also modify the location in the same file.

## Android

The requirements for services on Android are:

- For development it is recommended to use Android Studio. The latest version available can be downloaded [here](#).
- Android SDK version 26+

### **Verifier and Wallet (Android)**

This repository contains the mobile application to verify certificates through Android. In order to install this project you must first clone it locally with the following command:

```
$ git clone
https://github.com/eu-digital-green-certificates/dgca-verifier-app-
android
```

In order to have the connection and certificate signing services, you must also have the core repository in the same folder, you can use the same command used to clone the core repository.

```
<project folder>
|__dgca-verifier-app-android
|__dgca-app-core-android
|__dgc-certlogic-android
```

Once you have the repositories installed, they must modify the verifier-context.jsonc file with the correct national system values. This file is located in the “app / src / acc / assets” folder. You must generate a file called "config.json" in the same folder and fill in the appropriate values as shown in the following diagram:

## Verifier

```
{ // Origin in ISO alpha 2 code:
  "origin": "XX",
  "versions": {
    "default": {
      "privacyUrl": "https://<PRIVACY_URL>",

      "context": { "url":
        "https://<URL_VERIFIER_SERVICE>/context",
        "pubKeys": [<PUBLIC_KEYS>]
      },
      "endpoints": {
        "status": { "url":
          "https://<URL_VERIFIER_SERVICE>/signercertificateStatus",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "update": { "url":
          "https://<URL_VERIFIER_SERVICE>/signercertificateUpdate",
          "pubKeys": [<PUBLIC_KEYS>]
        },
      },
      "countryList": { "url":
        "https://<URL_BUSINESSRULE_SERVICE>/countrylist",
        "pubKeys": [<PUBLIC_KEYS>]
      },
      "rules": { "url":
        "https://<URL_BUSINESSRULE_SERVICE>/rules",
        "pubKeys": [<PUBLIC_KEYS>]
      },
      "valuesets": { "url":
        "https://<URL_BUSINESSRULE_SERVICE>/valuesets",
        "pubKeys": [<PUBLIC_KEYS>]
      }
    }
  },
}
```

## Wallet

```

{ // Origin in ISO alpha 2 code:
  "origin": "XX",
  "versions": {
    "default": { "privacyUrl":
      "https://<PRIVACY_URL>",
      "context": { "url":
        "https://<URL_ISSUANCE_SERVICE>/context",
        "pubKeys": [<PUBLIC_KEYS>]
      },
      "endpoints": {
        "claim": { "url":
          "https://<URL_ISSUANCE_SERVICE>/dgci/wallet/claim",
          "pubKeys": [
            "1KdU1EbQubxyDDm2q3N8Kc1Z2C94Num3xXjG0pk+3eI=",
            "r/mIKG3eEpVdm+u/ko/cwxzOMo1bk4TyHI1ByibiA5E="
          ]
        },
        "countryList": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/countrylist",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "rules": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/rules",
          "pubKeys": [<PUBLIC_KEYS>]
        },
        "valuesets": { "url":
          "https://<URL_BUSINESSRULE_SERVICE>/valuesets",
          "pubKeys": [<PUBLIC_KEYS>]
        }
      }
    },
  },
}

```

In the file "app/src/main/java/dgca/verifier/app/android/di/NetworkModule.kt" modify the variable "BASE\_URL" by the url of the verifier:

```
const val BASE_URL = "https://<URL_VERIFIER_SERVICE>/"
```

In the case of the wallet, change it to:

```
const val BASE_URL = "https://<URL_ISSUANCE_SERVICE>/"
```

To run the project in an android emulator you must execute this command:

```
$ gradlew -PCONFIG_FILE_NAME="config.json"
```

## Frequent questions

This section describes the most frequently asked questions related to the project

- If I am using the issuance-web, how can I add authentication or some access restriction measure?

The issuance web application (issuance-web) does not have its own authentication system or any access control measure. This means that once this application is deployed, any user with access to the server can use it and issue certificates. There are different strategies to control access depending on the complexity and amount of resources that the countries have.

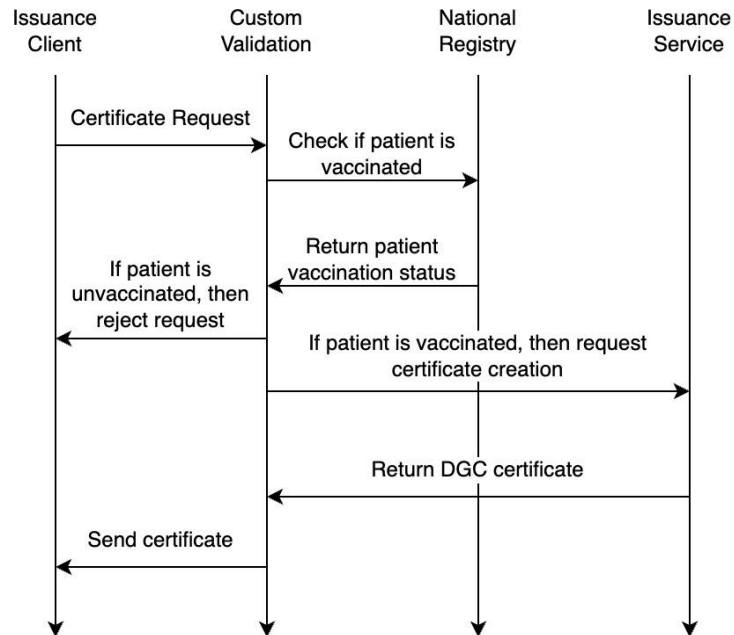
The simplest alternative to implement is to add basic HTTP authentication to the proxy server either nginx or apache. Both provide plugins to add this type of authentication, for example by configuring the .htpasswd file.

The next recommended option is not to use the issuance-web service and develop your own application that uses the issuance-service API. This way you have full control of development and you can add authentication at the application level.

In any case, it is recommended that the application is only visible for a specific segment of IPs or locations to avoid other types of traffic.

- If I have a national registry of vaccinated people, how can I integrate this information into the system?

Countries with a National Vaccination Registry can connect the information of vaccinated people to LACPASS through the issuance-service API. It is recommended to create software that is inserted between the certificate issuance client (issuance-web or custom development) and the issuance-service. This software should verify the authenticity of the certificate requested to be issued with the national registry and continue with the issuance process or reject it in case the requested data does not match. The following diagram exemplifies the operation.



- What are the steps to follow to be able to integrate with the EU?

The integration process is explained in the following link: [Onboarding Checklist](#).

In general, the process consists of sending the public keys to the EU to add them to the gateway database as explained in the gateway section. And after testing that everything is working correctly, you need to change the gateway endpoint to their official endpoint.

Ellos tienen a disposición 3 ambientes: Test, para las pruebas de integración (este ambiente sólo se inicia cuando se empieza el proceso de Onboarding, antes de eso está apagado). Acceptance, para probar y para que la UE valide que la integración funciona correctamente. Producción: ambiente que contiene los datos reales, una vez integrado a este ambiente se completa el proceso.

- How to handle people who are vaccinated for the first time and people who are already vaccinated?

It is recommended that countries that have implemented a National Vaccination Registry have integrated it using the instructions above. In this way, the custom validation layer that will be developed can handle cases in which people have already been vaccinated, have been vaccinated for the first time or have an incomplete vaccination schedule.

## Annex 2- Conectaton LACPASS Test Cases

### Test Cases

#### 1.1 General Objective:

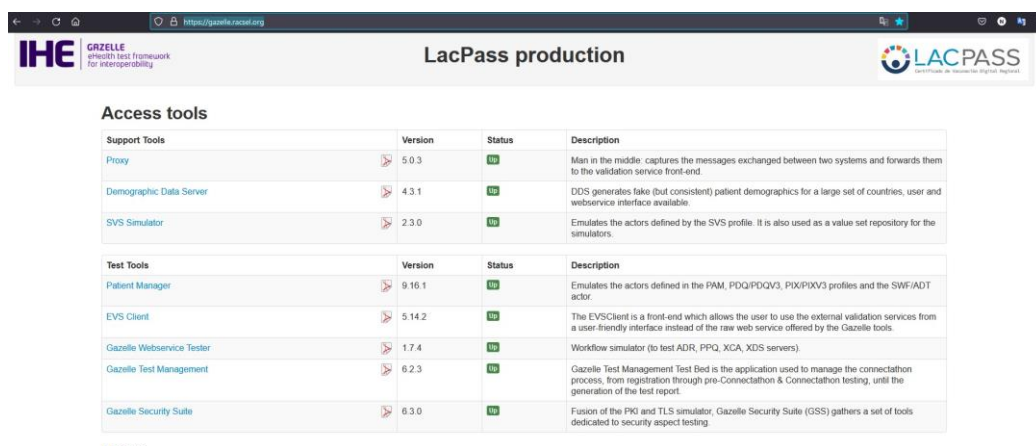
Develop technical activities to demonstrate that it is currently feasible for the different country information systems to access, exchange, integrate and cooperatively use the data associated with COVID-19 certificates, through the use and interaction with the LACPass regional directory services -which is based on the EU DCC definition- and the IHE Gazelle testing platform.

#### 1.2 Specific objectives:

1. Create and issue COVID-19 digital certificates according to EU-DCC standard.
2. Validate the certificates issued within the same country with the Gazelle platform.
3. Peer verification of COVID-19 certificates issued by participants.

#### 1.3 Methodology:

1. Generation of certificates according to EU-DCC from each local platform. Data for test cases by definition must come from the same local systems.
2. Use of the Gazelle platform for the validation and traceability of the defined test cases. Gazelle platform available on: <https://gazelle.racsel.org/> (figure 01).



The screenshot shows the IHE Gazelle Platform web interface. The page title is "LacPass production". Below the header, there is a section titled "Access tools" which contains two tables. The first table lists "Support Tools" and the second table lists "Test Tools".

Support Tools	Version	Status	Description
Proxy	5.0.3	UP	Man in the middle: captures the messages exchanged between two systems and forwards them to the validation service front-end.
Demographic Data Server	4.3.1	UP	DDS generates fake (but consistent) patient demographics for a large set of countries, user and webservice interface available.
SVS Simulator	2.3.0	UP	Emulates the actors defined by the SVS profile. It is also used as a value set repository for the simulators.

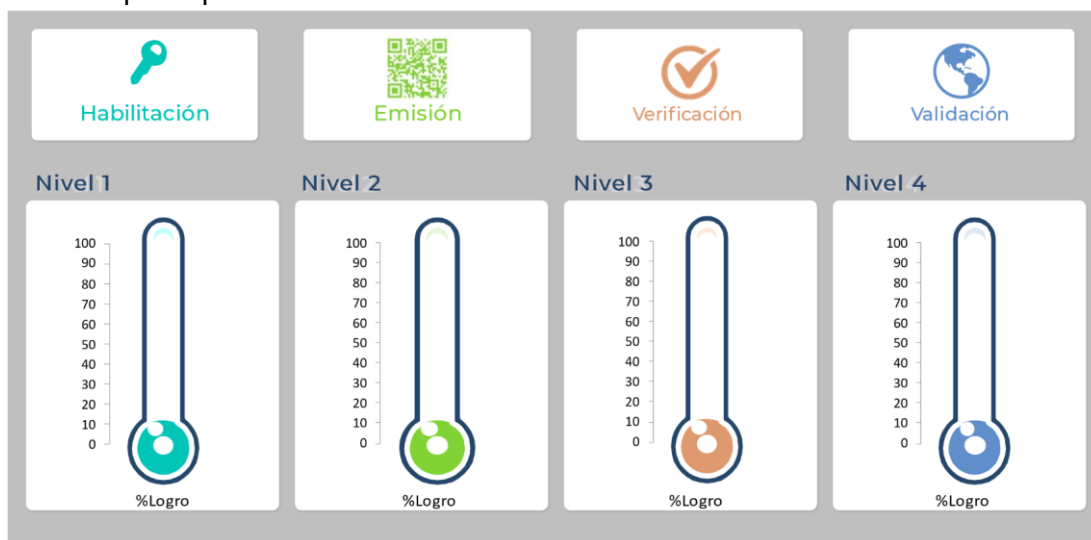
  

Test Tools	Version	Status	Description
Patient Manager	9.16.1	UP	Emulates the actors defined in the PAM, PDQ/PDQV3, PIX/PIXV3 profiles and the SWFI/ADT actor.
EVS Client	5.14.2	UP	The EVSClient is a front-end which allows the user to use the external validation services from a user-friendly interface instead of the raw web service offered by the Gazelle tools.
Gazelle Webservice Tester	1.7.4	UP	Workflow simulator (to test ADR, PPQ, XCA, XDS servers).
Gazelle Test Management	6.2.3	UP	Gazelle Test Management Test Bed is the application used to manage the connection process, from registration through pre-Connection & Connection testing, until the generation of the test report.
Gazelle Security Suite	6.3.0	UP	Fusion of the PKI and TLS simulator, Gazelle Security Suite (GSS) gathers a set of tools dedicated to security aspect testing.

Fig.01: IHE Gazelle Platform.

3. All the test cases of the Conectaton LACPASS are available and detailed on the Gazelle platform.
4. Four levels of compliance will be assessed for all participants:
  - a. **Level 1 - Enablement:** Corresponds to the correct configuration of the trust frameworks, correctly upload and download the public keys for the validation of COVID certificates.
  - b. **Level 2 - Issuance:** Corresponds to the correct generation and issuance of COVID certificates from each of the local systems of the participants.
  - c. **Level 3 - Verification:** Corresponds to the correct verification through the Gazelle platform, of the COVID certificates issued from each country
  - d. **Level 4 - Validation:** Corresponds to the peer validation of COVID certificates issued by each country, this test case is repeated n times for each participant to be validated between peers.

Figure 01 below graphically shows compliance monitoring levels for all LACPASS Conectaton participants.



*Fig.01: Compliance levels associated with the LACPASS Conectaton test cases.*

#### 1.4 List of Conectaton LACPASS test cases:

The totality of test cases, their detail and definition are available on the Gazelle platform.

Table 01 below details the test cases to be executed with the corresponding link to their description:

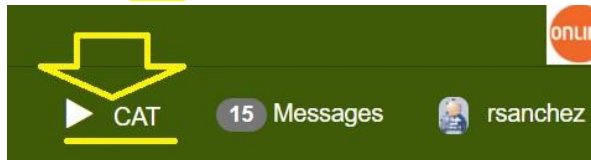
<b>Tests</b>	<b>Nombre de Test</b>	<b>Link a la descripción del Test</b>
Test 1	DCC - Recovery Certificate*	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=74">https://gazelle.racsel.org/gazelle/test.seam?id=74</a>
Test 2	DCC - Result Certificate*	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=76">https://gazelle.racsel.org/gazelle/test.seam?id=76</a>
Test 3	DCC - Vaccination Certificate	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=75">https://gazelle.racsel.org/gazelle/test.seam?id=75</a>
Test 4	DCC - Validation Error Case	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=70">https://gazelle.racsel.org/gazelle/test.seam?id=70</a>
Test 5	DCC - Scan Digital Certificate (Chile)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 6	DCC - Scan Digital Certificate (Colombia)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 7	DCC - Scan Digital Certificate (Ecuador)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 8	DCC - Scan Digital Certificate (El Salvador)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 9	DCC - Scan Digital Certificate (Paraguay)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 10	DCC - Scan Digital Certificate (Perú)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 11	DCC - Scan Digital Certificate (Suriname)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 12	DCC - Scan Digital Certificate (Uruguay)	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>

**Table 01: List of Test Cases.**

Test cases marked with \* (Test 1 and 2) are only required for those countries that are currently able to issue Test and Recovered certificates. For cases of peer validation, the verification of your own certificate (Test 5 to 12) does not apply.

# Test Instance Execution Guide

- **Step 1:** Go to the **CAT** menu



- 

**Step 2 :** Search for the test you want to execute then click on the **+** button

Sys	Profil	Acteur	Option de profil	Type	R/O
OTHER_DHE_MHD	DCC	CERTIFICATE_CONSUMER	NONE	T	2/0
Test			Meta Test		
DCC - Scan Digital Certificate				<b>+</b>	R / 7
DCC - Validation Error Case				<b>+</b>	R / 1

- **Step 3:** Select your country certificate you want to test by clicking on the **+** button

## Start test instance

DCC - Scan Digital Certificate Configuration

Role	Systems
	Organization Name      System keyword
<b>+</b> CERTIFICATE_CREATOR [1,1] ?	
0 Participants	
<b>✓</b> CERTIFICATE_CONSUMER [1,1] ?	
DHE	OTHER_DHE_MHD

The list of countries certificates will be displayed

**Step 4:** Select one of them, then click on Add

Select partner system(s) for the role : CERTIFICATE\_CREATOR

Card min: 1  
Card max: 1  
Systems :

- OTHER\_DHE\_MHD
- OTHER\_MINSAL(Chile)\_MeVacunoDCC
- OTHER\_MINSAL\_Certificados
- OTHER\_MINSAPERU\_COVID
- OTHER\_MOHS\_CPS

⇒ Add all

→ Add

← Remove

⇐ Remove all

Add selected partner(s)

- **Step 5:** Then click on the button « Add selected partner(s) »

Select partner system(s) for the role : CERTIFICATE\_CREATOR

Card min: 1  
Card max: 1  
Systems :

- OTHER\_DHE\_MHD
- OTHER\_MINSAL(Chile)\_MeVacunoDCC
- OTHER\_MINSAL\_Certificados
- OTHER\_MINSAPERU\_COVID
- OTHER\_MOHS\_CPS

⇒ Add all

→ Add

← Remove

⇐ Remove all

- **Step 6:** Start a new test instance by clicking on the green button

Select partner system(s) for the role : CERTIFICATE\_CREATOR

Card min: 1  
Card max: 1  
Systems :

- OTHER\_DHE\_MHD
- OTHER\_MINSAL(Chile)\_MeVacunoDCC
- OTHER\_MINSAL\_Certificados
- OTHER\_MOHS\_CPS

⇒ Add all

→ Add

← Remove


⇐ Remove all


Add selected partner(s)

**Step 7:** Run the test instance

## Start test instance

DCC - Scan Digital Certificate Configuration

Role	Systems					
	Organization Name	System keyword	Integration profile	Actor	Table	Action
✓ CERTIFICATE_CREATOR [1,1] ⓘ	MINSAPERU	OTHER_MINSAPERU_COVID	DCC	CERTIFICATE_CREATOR		
<small>1 Participants</small>						
✓ CERTIFICATE_CONSUMER [1,1] ⓘ	DHE	OTHER_DHE_MHD	DCC	CERTIFICATE_CONSUMER		
<small>1 Participants</small>						



# Add permalink in your tests

Prerequisite: Validate a certificate in QR Code Validator tool


- **Step 1:** Validate your certificate and then copy the permanent link

External Validation Service Front-end

IHE ▾ Lacpass ▾ Add-ons ▾ Administration ▾

## DGCG QR Code Validator

Information

**Filename :** gateway\_valid\_qr.jpg 




**Standard :** LACPASS Validator

**OID :** 1.3.6.1.4.1.12559.11.47.468

- **Step 2:** Go back to your test instance. At the bottom of the page, click on the globe to add the permanent link as a proof.

**Desc:** Please see notes in the Evaluation section above

**40** **Logs:** No comment, file or URL

   Upload a file (click or drop)

Proxy messages

Step	Trans.	Opt.	Sending Actor	Receiving Actor

