

## Documento de Relatoría

*Componente 1 LACPASS*

RED AMERICANA  
DE COOPERACION  
SOBRE SALUD  
ELECTRONICA



Introducción	4
Evolución del Bien Público Regional	5
Conectaton LACPASS	12
Objetivos	12
Misión	12
Desarrollo Conectaton	13
Casos de Prueba	15
Resultados	16
Encuesta Conectaton LACPASS	20
Pasos hacia el futuro.	25
Conclusiones de Conectaton	27
Lecciones Aprendidas	28
Anexos	29
Anexo 1- Documentación Técnica LACPASS	29
Emisión	31
Implementación	33
Tecnologías	33
Requisitos del Servidor	33
Pre-requisitos	33
Vaccination Entry (“v”)	40
Test Entry (“t”)	40
Recovery Entry (“r”)	40
Aplicaciones Móviles de Verificación	46
IOS	47
Verifier	47
Wallet	48
Android	49
Verifier y Wallet (Android)	49
Preguntas Frecuentes	52
Anexo 2- Casos de Prueba Conectaton LACPASS	54
Casos de Prueba	54
Guía ejecución instancia de prueba	57
Añadir enlace permanente en sus pruebas	59



# Introducción

Las modificaciones producidas por la pandemia de COVID-19 aceleró muchos procesos, principalmente al nivel de los Sistemas de Información en Salud, se tuvieron que modificar de forma rápida la forma en brindar atención médica porque se debía de cambiar la modalidad de esta.

También debido a la cantidad de información que se genera por medio de la realización de las Pruebas COVID-19, la vacunación produjo que los países empezarán a organizar dicha información para que la misma sea accesible de forma rápida para la población, así como para las autoridades sanitarias.

Posteriormente el avance de la vacunación demostró un control de la pandemia con disminución de los casos y de la mortalidad, como consecuencia de las rápidas campañas de vacunaciones empleadas en los distintos países, así comenzó a visualizarse la posibilidad de realizar las aperturas de fronteras cumpliendo con las pautas sanitarias impuestas por los distintos países, generando la necesidad de la utilización de los Certificados COVID-19 como forma de garantizar la situación de salud de la persona.

Los países comenzaron con el desafío de la digitalización permitiendo una rápida accesibilidad por parte de las personas e Instituciones de la Salud, muchos países comenzaron con dicha utilización a nivel nacional, permitiendo que las personas pudieran realizar actividades mediante la utilización de dichos certificados digitales, y posteriormente incluirlos dentro de la documentación requerida en cruces fronterizos.

El pionero en la implementación de los certificados para realizar viajes transfronterizos fue la Unión Europea, los países miembros comenzaron a realizar la verificación y validación de estos. De esta forma se pudo realizar la apertura de frontera entre los países miembros garantizando el estado de salud de las personas que transitaban de un país a otro. Posteriormente la UE permitió que países que no pertenecen a la UE pero que cumplen con los requisitos del EU-DCC puedan acceder a circulación dentro de la UE.

El modelo implementado por parte de la UE generó la posibilidad de implementación en América Latina y el Caribe<sup>1</sup> produciendo después de mucho trabajo la realización en Santiago de Chile de la primera Conectaton de América Latina y el Caribe.

---

<sup>1</sup> Ver Anexo 1- Documentación Técnica



- Decidir la incorporación de nuevos países.

Y dentro de las definiciones de las cuales se encargan el comité técnico encontramos:

- Definición de estándares y arquitectura.
- Marco de confianza.

Al inicio del proceso se encontraban los siguientes países, de los cuales detallaremos su situación inicial a continuación:

- Argentina.
- Chile.
- Colombia.
- Paraguay.
- Surinam.
- Uruguay.

Al inicio del proceso se realizó una encuesta a todos los países participantes abarcando tres objetivos:

- Entendimiento: generar una interacción directa entre cada uno de los países participantes el cual permite conocer el nivel técnico que presenta cada uno de los países.
- Expectativas: conocer las expectativas de cada país respecto a su participación en dicho proyecto.
- Dialogo: permitir establecer un dialogo personalizado con cada uno de los equipos con el fin de disminuir las brechas y necesidades existentes en cada uno de ellos.

Como punto de partida del recorrido de la transformación digital de la región, se realizó una entrevista con cada uno de los representantes expertos de cada país para conocer su estado actual, la información recabada se agrupo en tres categorías y para los resultados de esta se elaboró una escala en la cual tomo los valores Alto, Medio y Bajo.

Las categorías en las que se agrupo las respuestas son:

- Visión del proyecto y participación: en la misma se pretendía conocer las expectativas del proyecto y sus plazos, en el cuál sería el nivel de participación Institucional, así como el nivel de los recursos humanos participantes.
- Estado de su sistema de vacunación actual: se buscaba conocer cuál era el nivel de madurez del registro nacional de vacunación que contaba el país, si se utilizaban estándares como FHIR y CIE-11, y si dichos certificados de vacunación se encontraban firmados digitalmente.
- Visualización de brechas y/o necesidades respecto de Perfiles IHE: el capital humano en salud digital y su arquitectura e infraestructura.

Dichas entrevistas arrojaron los siguientes resultados por cada uno de los países:

- Argentina: en la entrevista se manifestó estar alineado con la visión y expectativas el proyecto, los recursos humanos presentan un nivel técnico alto pero la dedicación de los recursos es compleja, no tienen en uso en ese momento el CIE-11 y presentan un

registro de vacunación centralizado el cual se encuentra actualizado con FHIR y los certificados se encuentran firmados digitalmente.

- Chile: refiere en la entrevista que presenta expectativas alineadas con el proyecto y sus plazos, y en ese momento se encontraba en definición la formalización de los participantes. Presenta un nivel técnico medio, presentaban un registro único encaminado a FHIR y firma digital y no se utilizaba CIE-11.
- Paraguay: las expectativas del proyecto y sus plazos se las considero adecuada, pero el tiempo de dedicación de los recursos es limitado. Presentaban un nivel técnico medio, con un registro único existente encaminado hacia FHIR y la firma digital, no presentan CIE-11.
- Surinam: respecto a las expectativas y plazo del proyecto fueron consideradas adecuadas y presentan un gran compromiso y participación alineada con el proyecto. Se encontraban con el despliegue digital nacional (DHIS2) encaminado hacia el uso de los estándares. Presentan necesidades en desarrollo hacia FHIR, firma digital y CIE-11.
- Uruguay: manifiesta una visión y expectativas alineadas al proyecto, el apoyo necesario para el BPR, nivel técnico alto, presentan mapeo de CDA3 a FHIR y no utilizan CIE-11. Existen dudas respecto de la arquitectura e infraestructura para la realización de las pruebas de concepto.

Al realizar un resumen global de las respuestas obtenidas de las entrevistas para cada una de las categorías encontramos el siguiente status:

- Visión del proyecto y su participación: encontramos que las expectativas de todos los países entrevistados se encontraban alineados con el proyecto y los plazos, además se manifestó un importante compromiso de participación, pero en periodo de formalización, y una compleja dedicación exclusiva al proyecto.
- Estado de su sistema de vacunación actual: se encontraron distintos niveles de maduración de los registros de vacuna a nivel nacional en cada uno de los países, respecto de los estándares se encontró que FHIR debe implementarse en todos los países con un grado de esfuerzo variable entre cada uno y una visualización bastante más compleja de implementación del CIE-11. Experiencia con firma digital o autoridades certificadoras en todos los países.
- Visualización de brechas y/o necesidades: perfiles IHE se encuentra en todos los países con diferente nivel de adopción, se deberá fortalecer el capital humano en salud digital, y existen inquietudes con la arquitectura disponible.

Dichas entrevistas permitieron conocer como era la situación respecto de los sistemas informáticos de salud de cada uno de los países, siendo un insumo fundamental en dichos procesos de transformación digital en la región.

Asimismo, desde el Comité técnico se elaboraron dos grupos los cuales tenían como objetivo la definición de dos aspectos fundamentales, a continuación, se realizará una descripción de las discusiones llevada a cabo por cada uno de los grupos técnicos.

Siendo fundamental en dichos grupos abarcar tres grandes ítems para el desarrollo del proyecto como son la Arquitectura y Estándares, Marcos de Confianza y la privacidad y seguridad de la información que se va a intercambiar.

El grupo uno realizó la discusión respecto del Modelo de datos en donde se trataron los siguientes temas:

### Header

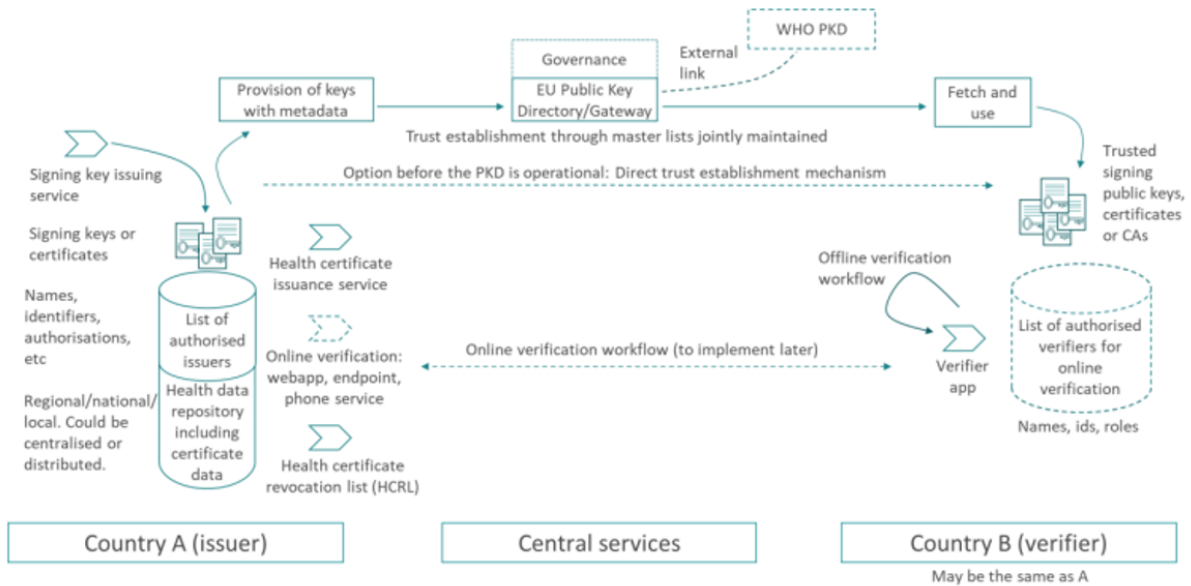
Data element	Description	Requirement status	Data type	Preferred code set
<b>Name</b>	The full name of the vaccinated person	Required	String	Not applicable
<b>Date of birth</b>	The individual's date of birth (DOB) if known. If unknown, use given DOB for administrative purposes. The full format of DD MM 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. If the <i>vaccine manufacturer</i> is unknown, <i>vaccine market authorization holder</i> is REQUIRED.	Required – Conditional	Coding	As defined by Member State
<b>Vaccine market authorization holder</b>	Name of the market authorization holder of the vaccine received. If <i>vaccine market authorization holder</i> is unknown, then <i>vaccine manufacturer</i> is REQUIRED.	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

- Revisión de la meta data.
- Estándares usados FHIR, CIE-11 y SNOMED CT.
- Ubicación del Modelo de información para el DDCC.
- Identificadores, español, lista de valores y semántica.
- Modelo de datos ALC.
- Adopción de CIE-11.
- Subsets.
- Lineamientos para la guía técnica y modelo de datos.

El segundo grupo técnico realizó la discusión sobre el modelo de intercambio que se iba a llevar adelante en el proyecto, y las definiciones fueron las siguientes:



- Identificación de los componentes para la arquitectura de intercambio de información, seguridad y firma electrónica.
  - Componentes.
  - Seguridad.
  - Firma.
  - Código QR.
  - Lineamientos de Guía Técnica de modelo de intercambio.

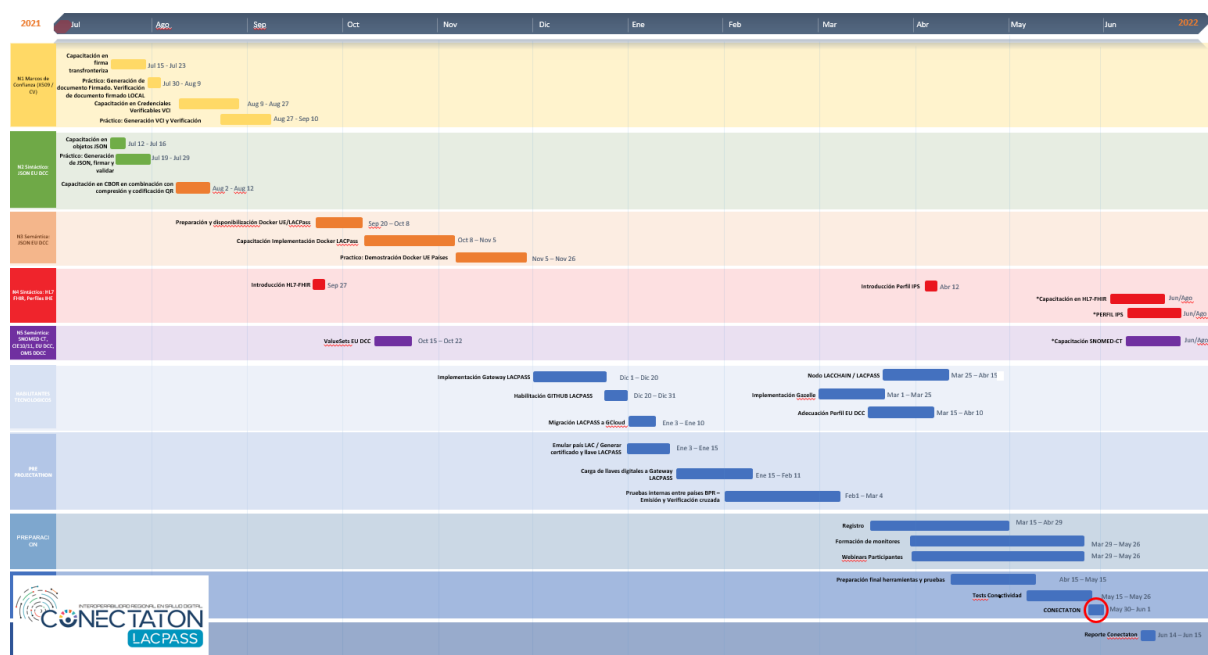
Otro aspecto a destacar el proyecto es el nivel estratégico definido el cual abarca tres aspectos fundamentales:

- Estándares: seguir los lineamientos de la OMS del DDCC y certificado de la UE.
- Alinearse a los planes estratégicos de la OPS: implementar sistemas digitales de salud e información abiertos, sostenibles e interoperables.
- Desarrollo y capacidades: fomentar el desarrollo de capacidades para poder utilizar la ciencia de datos y las tecnologías emergentes en la investigación, innovación, las políticas públicas y análisis ético en la salud pública.

Los cuales buscan tener los siguientes resultados:

- Estándares: poder desarrollar un proceso de aprendizaje y conocimiento vinculado a los estándares necesarios para los datos y marco de confianza.
- Infraestructura: implementación del Gateway regional.
- Pruebas de concepto: implementar las pruebas basadas en estándares de firma digital.
- Interoperabilidad: ejecutar una Projectathon que permita lograr dicha interoperabilidad a nivel regional.
- Escalabilidad: desarrollar informas técnicos el cual contenga las lecciones aprendidas, así como el análisis de la escalabilidad.

Pero todo el proceso de preparación de proyecto implica una serie de actividades más en la cual todos los países participantes deben estar presentes, para ello se realizó la planificación de dichas actividades en las cuales presentan plazos a cumplir durante el transcurso de todo el proyecto.



La presente planificación inicia en Julio 2021 en donde estas planteadas 10 etapas a cumplirse a lo largo del proyecto, las cuales además contienen cada una de ellas diferentes actividades a realizar.

Las 10 etapas propuestas en el GAM corresponden a:

- Nivel 1, Marco de confianza, XS09/CV.
- Nivel 2, Semántico JSON EU DCC.
- Nivel 3, Semántico, JSON EU DCC.
- Nivel 4, Semántico HL7, FHIR, Perfiles IHE.
- NS, Semántica SNOMED CT, CIE 10/11, EU DCC, OMS DDCC.
- Habilitantes tecnológicos.
- Pre Projectathon.
- Preparación.
- Projectathon.
- Post Projectathon.

Estas etapas serán desarrolladas entre Julio 2021 y junio 2022 aproximadamente, como se mencionó anteriormente cada una cuenta con distintas actividades a realizar, las cuales permitirán cumplir con los objetivos del proyecto, y dentro de las cuales hay algunas que significan un hito importante en la región.

Dentro de dichas actividades la capacitación sobre diferentes temas se encuentra siempre presente, ya que es fundamental brindarles a los países participantes la mayor cantidad de

conocimiento posible que les permite transitar el proyecto de la mejor forma posible, dichas capacitaciones se realizarán de forma teórica y prácticas para reforzar los conocimientos brindados.

La mayoría de las capacitaciones se realizaron en el periodo comprendido entre Julio y noviembre del 2021, donde se brindó toda la información técnica necesaria sobre temas como Firma Digital, generación de documentos firmados en forma local, sobre elementos y generación de JSON, CBOR y codificación QR, HL7 entre otras capacitaciones.

En septiembre del 2021 se incluye la preparación y disponibilización de Docker UE/LACPASS realizando capacitación teórica y práctica, agregando además el ValueSets EU DCC, generando así el logro del primer hito importante en el proyecto, en el cual ocurre en diciembre del 2021 con la implementación del Gateway LACPASS.

La implementación del Gateway demostró el avance de los países hasta ese momento y genero el inicio de nuevos desafíos que los países debieron enfrentar, una vez implementado se realizaron acciones relacionadas como la habilitación del GITHUB LACPASS, migración a GCloud junto con la emulación y generación de certificados y llaves LACPASS, para llevar a cabo esto se realizó en enero del 2022 la carga de las llaves digitales de los países al Gateway LACPASS.

Esta carga de llaves permite que se realicen las pruebas internas necesarias de emisión y verificación cruzada entre los países participantes.

Una vez realizada la implementación del Gateway se efectuaron las tareas relacionadas a los Nodos LACCHAIN/LACPASS, implementación de Gazelle y la adecuación a los perfiles de la EU DCC.

En el mes de marzo del 2022 se inició el proceso de registro, formación de monitores, Webinars y la preparación final, más la realización de un Test de conectividad previo a la realización de la Conectaton la cual se desarrolló del 30 de mayo al 1 de junio del 2022.

# Conectaton LACPASS

## Objetivos

Conectaton corresponde a una maratón de conectividad entre países para probar la interoperabilidad de los sistemas de información de Salud. Es un tipo de evento en el cual todas las organizaciones del sistema de salud pueden realizar las pruebas de conectividad e interoperabilidad en un ambiente controlado y neutral.

El encargado para ejecutar estas pruebas son los monitores, ellos se encargan de la validación y verificación durante el evento.

Persiguiendo como objetivo primordial fortalecer la capacidad de países de América Latina y el Caribe para enfrentar efectos del COVID-19 promoviendo la transformación digital en salud y a partir de allí avanzar en nuevos desafíos tecnológicos dentro de la región y poder lograr que al menos tres países puedan finalizar correctamente las pruebas planteadas para dicha Conectaton.

Se pretenderá demostrar por medio de pruebas prácticas y reales, que los distintos sistemas de información de los países participantes pueden intercambiar, integrar y usar de forma cooperativa los datos, con el objetivo a futuro del intercambio de datos asistenciales y telesalud entre los países de la región.

## Misión

Contribuir al fomento y adopción de tecnologías de información en salud, impulsando en forma colaborativa el desarrollo de capital humano dinamizando el ecosistema de innovación para mejorar la atención de salud de las personas.

Para ello se plantearon tres componentes a seguir, los cuales corresponden a:

- Mayores niveles de interoperabilidad para el intercambio de datos clínicos asistenciales: dicho componente fue el realizado en la presente Conectaton en el cual se establece los lineamientos de interoperabilidad de los certificados sanitarios COVID-19 en América Latina y el Caribe.
- Intercambio de datos para la vigilancia epidemiológica en Salud Pública a nivel Nacional y Regional.
- Crear los lineamientos y directrices para el desarrollo sostenible de la Telesalud.

## Desarrollo Conectaton

La Conectaton se realizó del 30 de mayo al 1 de junio en Santiago de Chile, el proyecto LACPASS (Ver Anexo 1) corresponde a una iniciativa de la Red Americana de Cooperación en Salud Electrónica de América Latina y el Caribe (RACSEL), el cual es patrocinado por el Banco Interamericano de Desarrollo (BID) y ejecutado por el Centro Nacional en Sistemas de Información en Salud (CENS) siendo quien lleva adelante este bien público.

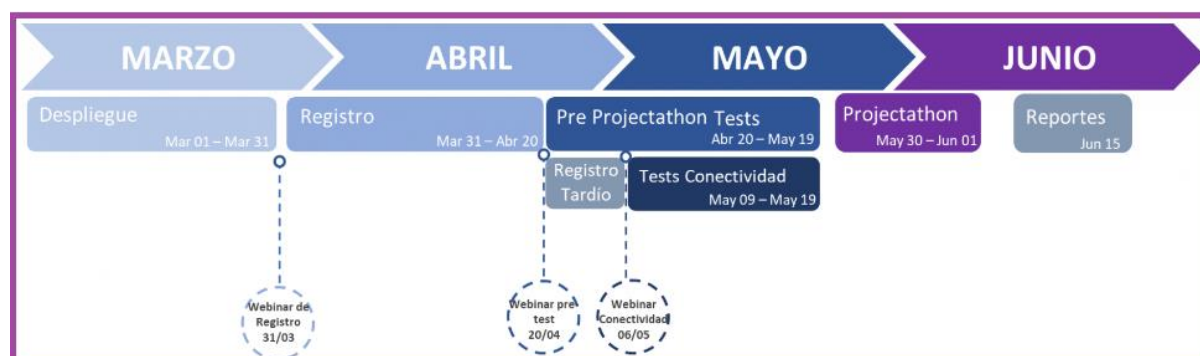
LACPASS está basado en el Certificado verde digital de la Unión Europea (UE DGC) en el cual corresponde a un repositorio de código abierto donde es usado por los países miembros de la UE, además se encuentra disponible en varios idiomas permitiendo así la accesibilidad al repositorio. Al conectar a todos los países interesados a LACPASS es posible usar esta tecnología para conectarse a la UE DGC.

Debido a esto, el proyecto LACPASS permite que, en la realización de viajes transfronterizos los certificados emitidos por el país de residencia puedan ser verificado en cualquiera de los países perteneciente al proyecto.

En la misma participaron los siguientes países como participantes: Chile, Colombia, Ecuador, El Salvador, Paraguay, Perú, Surinam y Uruguay. Los países observadores de la Conectaton fueron Bolivia, y Costa Rica.

Para poder llegar a la instancia de la Conectaton se llevó adelante una agenda de Projectathon en la cual los países participantes debieron de pasar una serie de etapas para poder finalmente participar en la Conectaton, cabe recordar que Argentina es parte del bien público, pero no participo en la Conectaton.

Una Projectathon corresponde a un evento de prueba uno a uno, en el cual se utilizan las mismas herramientas en una Conectaton en donde se permite probar diferentes perfiles IHE (Integrating the Healthcare Enterprise), de esta forma se persigue disminuir los riesgos existentes durante el proceso de implementación, porque se realizaron las pruebas necesarias previamente.



La Projectathon presenta las siguientes etapas, las cuales corresponden a:

- Registro; proceso en el cual todos aquellos que deseen participar deberán completar el proceso de registro.
- Pruebas Pre Projectathon; es el periodo en el cual se realizan pruebas con el fin de realizar una familiarización con las distintas herramientas.
- Conectividad; corresponde al proceso mediante el cual se realiza la verificación de la conectividad, si el sistema está listo para la realización de las pruebas reales, y es el monitor quien confirma si la prueba fue o no exitosa.

El encargado de verificar y de calificar cada una de las pruebas realizadas es el monitor y es quien determina si la prueba fue realizada como se esperaba.

La herramienta que se utilizó para gestionar las pruebas de interoperabilidad es Gazelle <https://gazelle.racsel.org/> en dicha página se encuentra toda la información técnica necesaria para la realización de estas.

Los dos primeros días se llevaron a cabo las pruebas de conectividad de los distintos países, el monitor es quien va a ir evaluando el desarrollo de estas y validar finalmente si se desarrolló satisfactoriamente.

Las pruebas realizadas por parte de los países participantes correspondían a la generación, emisión, validación de los certificados y el intercambio de los certificados entre los participantes, el documento de las pruebas realizadas se encuentra en el Anexo 2 del presente documento.

A continuación, se realizará una descripción de las pruebas realizadas, así como los resultados obtenidos por parte de los participantes.

## Casos de Prueba

Los casos de prueba<sup>2</sup> corresponden a actividades técnicas que permiten demostrar que es viable que los distintos sistemas de información de salud de los países participantes puedan acceder, intercambiar, integrar y utilizar de manera cooperativa los datos asociados a los certificados COVID-19, por medio de la utilización de los servicios de LCPASS en el cual se encuentra definido según lo establecido para la EU-DCC y Gazelle de IHE.

Los países participantes durante la Conectaton deberán ser capaces de:

- Crear y emitir certificados COVID-19, según definición realizada por EU-DCC.
- Validar los certificados emitidos dentro del mismo país utilizando la plataforma Gazelle.
- Verificar entre los países certificados COVID-19 emitidos por los participantes.

Entre todos los participantes se realizará la evaluación de cuatro niveles de cumplimiento de las pruebas:

- Nivel 1 – Habilitación: corresponde a la configuración correcta de los marcos de confianza, cargar y descargar de manera correcta las llaves públicas para la validación de los certificados COVID-19.
- Nivel 2 – Emisión: corresponde a la correcta generación y emisión de los certificados COVID-19 desde cada uno de los sistemas participantes.
- Nivel 3 – Verificación: corresponde a la correcta verificación mediante la plataforma Gazelle, de los certificados COVID-19 emitidos desde cada uno de los países participantes.
- Nivel 4 – Validación: corresponde a la validación entre pares de los certificados COVID-19 emitidos por cada país, este caso de prueba se repiten N veces por cada participante que deberá ir validando entre pares.

Dentro del documento Conectaton LCPASS Casos de prueba ubicados en el Anexo 2 podrán visualizarse los detalles técnicos de las pruebas.

---

<sup>2</sup> Ver Anexo Casos de Prueba

## Resultados

Posteriormente, de dos días de pruebas entre los países participantes se obtuvieron los datos que serán detallados a continuación.

Durante la Conectaton se ejecutaron un total de 83 pruebas, de las cuales se obtuvieron los siguientes resultados:

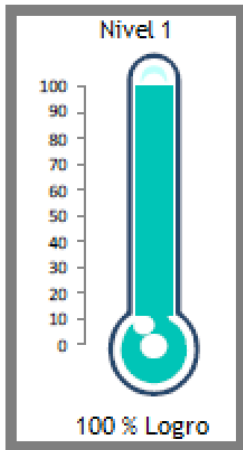
- 83% de las mismas finalizaron correctamente, correspondiendo a un total de 68 pruebas.
- 10 % no pudieron ser finalizadas correctamente, correspondiendo a un total de 8 pruebas.
- 7 % de las pruebas fracasaron, correspondiendo a un total de 7 pruebas.



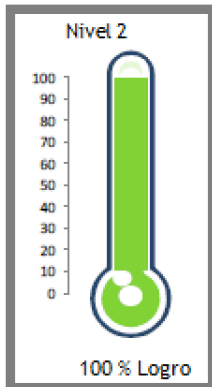
Es importante señalar que la realización de todas las pruebas debía de cumplirse en un periodo de tiempo determinado, por lo que todas aquellas pruebas que pudieran haber finalizado correctamente fuera de dicho periodo de tiempo no se validaba como finalizadas correctamente.

En el caso de las pruebas que no pudieron finalizar correctamente debido a problemas de conectividad, los cuales fueron ocasionados por una sobrecarga de dispositivos conectados en forma conjunta generado que se produjeran caídas de la red.

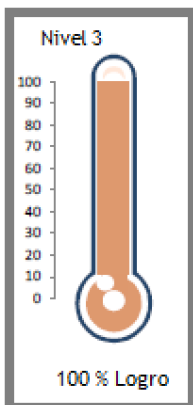
Tomando en cuenta los cuatros niveles de evaluación planteados previos a la realización de las pruebas, se obtuvieron los siguientes resultados.



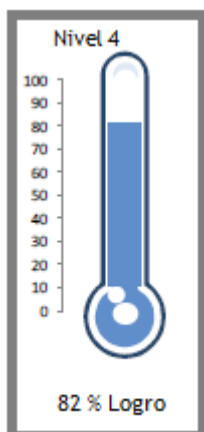
Respecto del primer nivel de evaluación el cual corresponde a la Habilitación, los países fueron capaces de compartir sus llaves (firmas) así como cargar y descargar la de los otros países en un 100 % de las pruebas realizadas.



Respecto del segundo nivel de evaluación el cual corresponde a la Emisión, para la realización de dichas pruebas se tomaron los estándares planteados por la EU-DCC, los países fueron capaces de realizar la emisión de los certificados en el 100 % de las pruebas realizadas.



Respecto del tercer nivel de evaluación el cual corresponde a la Verificación, los certificados generados y cargados en la plataforma correspondiente corresponden a certificados válidos en el 100 % de las pruebas realizadas.



Respecto del cuarto nivel de evaluación el cual corresponde a la Validación, la validación debía de realizarse en un periodo de tiempo determinado y una vez cumplido el mismo no se permitía seguir ejecutando dicha validación, siendo el resultado de la presente prueba de Validación de un 82% de las pruebas realizadas.

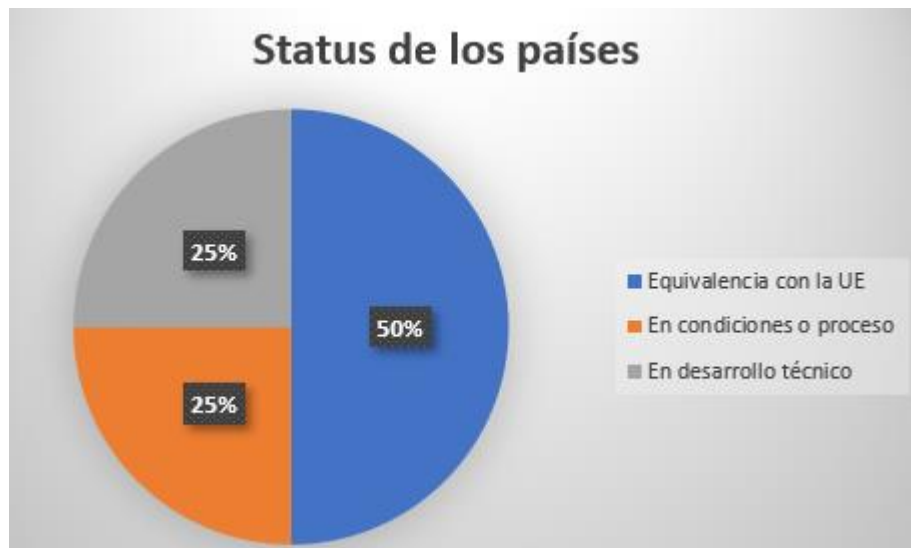
Una vez terminadas las pruebas de la Conectaton LACPASS podemos conocer el status de los países participantes respecto a la equivalencia de la UE:

PAIS	Repositorio Centralizado	Esquema JSON	Subsets EU	CBOR / COSE	FIRMA	Validador	UE Equivalente
	Si	Equivalente	A Desarrollar	---	PKI	---	
	Si	Equivalente	Equivalente	Equivalente	CV/PKI	Ok	
	Si	Equivalente	Códigos Propios	En ambiente Test	PKI (Test)	En ambiente Test	
	Si	Equivalente	Códigos Propios	Equivalente	En Desarrollo	En Desarrollo	
	Si	Equivalente	Equivalente	Equivalente	PKI	Ok	
	Si	Equivalente	Equivalente	Equivalente	PKI	Ok	
	Si	Equivalente	Equivalente	Equivalente	PKI	Ok	
	En Desarrollo	En ambiente Test	En ambiente Test	En ambiente Test	PKI	En ambiente Test	
	Si	Equivalente	Equivalente	Equivalente	PKI	Ok	

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

En donde encontramos que cuatro países presentan hoy una equivalencia con la UE, dos se encuentran en desarrollo técnico y dos en proceso o condiciones de validar dicha equivalencia. Es importante señalar que finalmente Argentina no participó del evento.

Gráficamente el status se ve de la siguiente manera



# Encuesta Conectaton LACPASS

Desde la organización de la Conectaton LACPASS se definió una vez finalizado el encuentro realizar entre los países participantes una Encuesta para conocer la opinión de todo el proceso realizado hasta la realización de la Conectaton.

La encuesta se dividió en tres bloques, con el primer bloque se pretende conocer el estado en el cual se encontraba cada uno de los países participantes frente a los Certificados COVID-19, teniendo en cuenta que la meta es llegar el mismo estado que tiene hoy la Unión Europea respecto a los Certificados COVID-19.

Un segundo bloque correspondiente a preguntas relacionadas al evento, si presentaron inconvenientes en cada uno de los niveles, así como conocer la opinión respecto de las charlas brindadas durante la realización de la Conectaton LACPASS y los insumos brindados con información técnica.

En el tercer bloque nos interesó conocer aspectos como mejoras que puedan realizarse en futuros eventos de características similares para poder reforzar la calidad de este tipo de eventos a nivel Regional, finalmente solicitamos a los encuestados una reflexión final la cual enriquecerá aún más con eventos realizados en América Latina y el Caribe.

A continuación, se realizará un análisis de las respuestas obtenidas en la Encuesta, la misma fue respondida por 8 países Chile, Colombia, Ecuador, El Salvador, Paraguay, Perú, Surinam y Uruguay.

Respecto de los Certificados COVID Digitales la situación entre los países varía entre los tres tipos de certificados existentes, en el caso de los Certificados de Vacuna COVID-19 encontramos que todos los países presentan la digitalización de este en diferentes status, encontrando tres países con certificados homologados por la UE, el resto de los países presentan Certificados de Vacunas digitales con código QR y firma digital avanzada.

En el caso de los Certificados de Recuperados la situación no es la misma entre los distintos países, solamente un país cuenta con este Certificado Homologado por la UE, en el caso de los demás países la situación es que no cuentan con dicho Certificado o en caso de tenerlo en forma digital el mismo solo es utilizado por parte de los prestadores y no está disponible para la población en general.

Finalmente, en el caso de los Certificados de Resultado de Pruebas Digitales encontramos que solamente un país cuenta con el Certificado Homologado por parte de la UE, el resto de los países solamente dos países cuentan con certificados digitales que se encuentran disponible para la población en general por medio de aplicaciones propias en dichos países.

Posteriormente con la encuesta se intentó conocer no solo la percepción que se tenía previa a la realización del evento, sino que además se consultó sobre la opinión acerca de los materiales, charlas la información técnica previa a la realización de la Conectaton LACPASS.

Respecto de la percepción previa a la realización evento todos los países participantes coincidieron en la importancia del aprendizaje sobre la experiencia y estado de los demás países respecto de sus Certificados Digitales.

Además de poder realizar las distintas pruebas de conectividad entre los países permitiendo así el aprendizaje en conjunto ya que muchos presentaban desconocimiento acerca de las pruebas y el estado en el cual se encontraban los demás países.

La mayoría de los países no presentaron inconvenientes previos a la realización del evento, pero aquellos que, si presentaron inconvenientes, mencionaron que fueron los siguientes:

- Inconveniente para subir las claves públicas mediante el uso del servicio Gateway, inconveniente solucionado satisfactoriamente.
- Inconveniente para realizar la conexión al Gateway, inconveniente solucionado satisfactoriamente.
- Inconvenientes relacionados al viaje y viáticos siendo propios del país y no relacionado al evento.

Cuando le consultamos a los países participantes sobre su opinión referente a las charlas, Webinar, material técnico brindado por parte de la organización todos coincidieron en que el material brindado fue muy completo y de buena calidad brindando así la información necesaria para llevar adelante las pruebas solicitadas.

Sobre la opinión de las charlas brindadas se consultó la opinión específica sobre la información brindada del perfil IPS International Patient Summery en donde nuevamente todos los países coincidieron en la buena calidad de la información brindada sobre el IPS y destacaron la posibilidad de aprender sobre IPS para poder avanzar en el mismo en cada uno de los países.

En un segundo bloque de preguntas nos interesó conocer la opinión de los participantes durante la realización del evento, donde lo primero que nos interesó saber es si habían presentado algún inconveniente y en caso afirmativo que nos comentarán cual había sido.

Los participantes respecto de este punto manifestaron que solamente el primer día del evento presentaron inconvenientes de conexión a la red Wifi, los cuales fueron solucionados rápida y satisfactoriamente permitiendo continuar con el desarrollo de este sin más inconvenientes.

Para conocer específicamente el transcurso de las pruebas, se consultó a los participantes hacerse de si tuvieron algún tipo de inconveniente en cada uno de los niveles, donde obtuvimos las siguientes respuestas:

- Nivel 1- Habilitación: respecto a este nivel ningún país manifestó haber presentado algún inconveniente.
- Nivel 2- Emisión: respecto a este nivel ningún país manifestó haber presentado algún inconveniente.

- Nivel 3- Verificación: en este punto si se presentaron inconvenientes, puntualmente dos países manifestaron haber presentado inconvenientes con la verificación de los QR puntualmente con Uruguay.
- Nivel 4- al igual que lo mencionado anteriormente, dos países manifestaron problemas con la Validación de los códigos QR de Uruguay. Dicho inconveniente se relacionaba con la utilización de DGCA-App-Core-Android-Main que dificultaba la Validación de los códigos QR de Uruguay, generado por que las claves públicas de Uruguay no estaban en el servicio signercertificateStatus del Verifier, generándose que no se pudieran validar los QR de Uruguay.

Una vez finalizadas las pruebas se consultó a los participantes como evaluaban la sinergia lograda entre todos los países participantes durante la Conectaton LACPASS, en líneas generales todos los países evaluaron como excelente la sinergia generada, pero también se manifestó que no se generaron instancias puntuales de intercambio entre los países ya que cada una de las delegaciones se encontraban trabajando sobre sus pruebas.

Así como al inicio de la encuesta se consultó sobre el cual era el estado de los Certificados Digitales de COVID-19 en cada uno de los países participantes, también nos resultó de gran interés conocer una vez finalizado el evento cual sería la postura de los distintos países participantes sobre la implementación de dichos Certificados.

Donde encontramos una variedad de posturas frente a los mismos, los cual detallaremos a continuación:

- Certificado de Vacunación, aquí nos encontramos que tres países presentan homologación con la UE, el resto de los países se encuentran en proceso de desarrollo de los Certificados, o en proceso de implementación. Además de cumplir con los pasos que se requieren para lograr la homologación con la UE.
- Certificados de Recuperados de COVID-19, solamente un país cuenta con la homologación del certificado con el UE, cinco países no generan certificados digitales de Recuperados y el resto de los países generan certificados pero que los mismos son utilizados por parte de los prestadores de salud.
- Certificado de Resultado de Pruebas COVID-19: solamente un país emite certificados homologados por parte de la UE, hay tres países que tienen certificados digitales de resultados de pruebas COVID-19 y el resto no cuenta con dichos certificados.

También se realizó la consulta a los países participantes si pensaban realizar la implementación en productivo de los lineamientos planteados desde RACSEL o si consideraba que algún lineamiento no se podía llevar adelante, y en este caso todos los países coincidieron en la intención de implementar los lineamientos planteados por RACSEL y un solo país que actualmente se encuentra iniciando los trabajos para la implementación del IPS.

Como la Conectaton LACPASS fue el primer evento realizado para América Latina y el Caribe se les pidió a los participantes que nos indiquen posibilidades de mejoras para próximos eventos a realizarse de características similares, encontramos que el 55,5% países (corresponde a 5) indicaron que no tenían mejoras para plantear ante próximos eventos, el 45,5 % países (corresponde a 4) que si indicaron mejoras fueron las siguientes:

- Mejor conexión en la red WIFI.
- Tener información más clara relacionada con los viajes, viáticos y estadías.
- Ajustes técnicos previos relacionados a la Validación de los códigos QR, relacionado con que los países no podían realizar la lectura de los códigos QR de Uruguay.
- Inclusión en próximos eventos para poder realizar un caso con certificados digitales como el registro del evento, con esto los países participantes pueden utilizar dicha tecnología.

Para finalizar la encuesta les pedimos a los participantes de que nos compartieran una reflexión final de todo el proceso de la Conectaton LACPASS para cumplir con el objetivo planteado para la realización de las pruebas, a continuación, compartimos dichas reflexiones finales:

- Muchas cosas tecnológicamente se encuentran resueltas, es solo cuestión de voluntad.
- El evento fue muy enriquecedor, la experiencia de compartir logros, lecciones aprendidas y acciones en pro de transformar la Salud Digital en nuestros países, compartir retos y aprender de los errores de la región para no caer en los mismo, así como las buenas experiencias para poder implementarlas. Por medio de estos eventos se crea una comunidad que puede aportar ideas y apoyo cuando se requiere desde otro país. Ver los avances de la región motiva a trabajar más fuerte para no quedar atrás en la Transformación Digital.
- La organización y la modalidad de testeo cruzado entre los países fue muy amigable y fácil de usar.
- Ha sido un trabajo gratificante poder conocer la tecnología empleada en la UE y poder implementar algo así en nuestros sistemas nacionales.
- La gestión y reuniones preliminares para la Conectaton fueron fundamentales para alcanzar el éxito de las pruebas, por esta preparación, gestión y coordinación Felicitaciones. Lo único que les recomendaría es para la próxima contar con un canal de Internet de backup para evitar la incidencia que ocurrió el primer día de la Conectaton.
- Que se realicen de forma más consecutivo eventos como este a fin de implementar con más celeridad y en conjunto los países, tecnología que nos permita contar con la Historia Clínica Electrónica internacional.
- Fue un proceso muy organizado y con bastante preparación dado que desde diciembre se venía realizando la gestión de este.
- Fue una gran instancia para aprender, ver en qué se encuentran nuestros países vecinos y las miradas a futuro.
- La realización de las pruebas ayudo bastante contar con personal técnico que brindo asistencia durante todo el evento.

- Estas Iniciativas en Latinoamérica fomentan la Interoperabilidad en Salud y son motivantes para trabajar en ayuda de la población, muy importante la participación de los organismos internacional y el financiamiento del BID, una muy buena oportunidad para generar contactos y compartir experiencias de los aciertos y errores que tiene cada país, realmente quedo muy agradecido por la oportunidad de participar en el CONECTATON LACPASS.
- Se alcanzaron las metas importantes porque se pudieron validar certificados de los países de la región.

En líneas generales todos los países participantes destacaron la buena calidad del material técnico brindado en cada una de las instancias del evento, así como también las charlas brindadas, siendo un aspecto fundamental ya que la correcta calidad de la información permitió fomentar el interés de los participantes en los temas planteados.

## Pasos hacia el futuro.

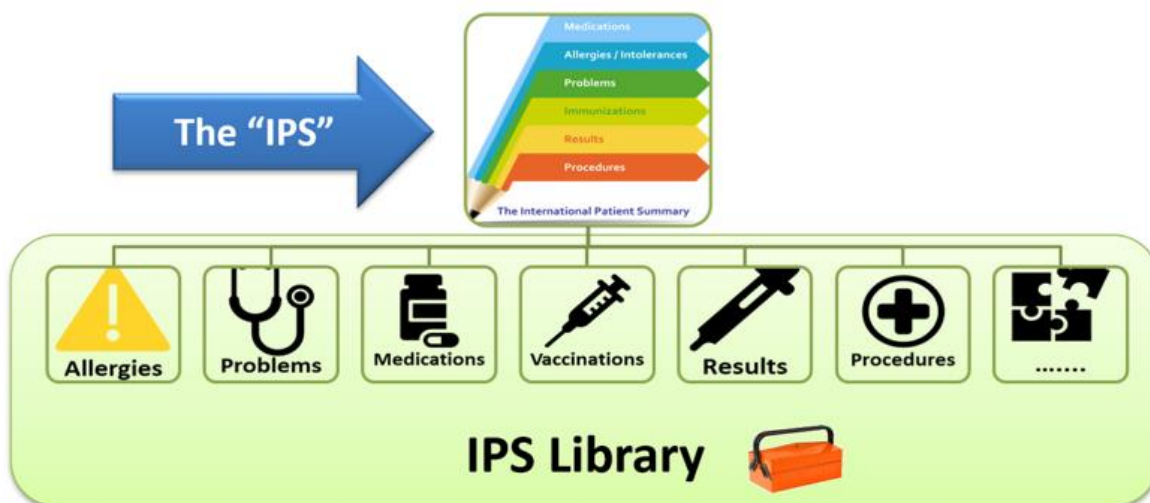
Es importante señalar que los resultados obtenidos en el transcurso de la Conectaton fueron favorables, se lograron cumplir los objetivos planteados de interoperabilidad entre los distintos países participantes.

Además de continuar avanzado al componente 02 del Bien Público Regional, iniciando con nuevos entrenamientos relacionados al avance hacia el próximo componente, dichos entrenamientos son:

- Formación en Gazelle.
- Perfil IPS.
- Perfil MDH.

Quedando habilitada nuevas instancias de interoperabilidad entre los países que permitan enfocarse en avanzar a la inclusión en la región del IPS.

Siendo el IPS Resumen Internacional del Paciente un sistema de datos clínicos no exhaustivo, el cual permite brindar atención personalizada en caso de urgencia y debe poder ser llevado junto con el paciente cubriendo todos los aspectos de privacidad y seguridad.



Siendo los componentes de este:



El alcance al cual se pretende llegar con el IPS corresponde a:

- Generar conocimiento sobre el IPS
- Generar conocimiento sobre FHIR
- Conocer su evolución hacia DDCC de la OMS
- Preparación de los casos de uso asociados a la interoperabilidad transfronteriza.
- Testear recursos de FHIR e IPS

## Conclusiones de Conectaton

Una vez finalizada la Conectaton y realizada la obtención de los resultados de las pruebas realizadas por parte de los países participantes se puede afirmar que los objetivos planteados son de que al menos tres países puedan llegar a completar la Conectaton fue cumplido satisfactoriamente. En el caso de El Salvador no pudo cumplir con los objetivos de la validación porque tuvieron demoras en la fecha límite, al pasar la fecha no se permite validar la prueba.

Es importante señalar que los Certificados Digitales de Vacunas COVID-19 se encuentran presentes en todos los países participantes con diferentes grados de evolución, algunos hasta se encuentran homologados con la Unión Europea, no se observa la misma situación con los certificados de Recuperados de COVID-19 y los certificados de Pruebas COVID-19.

Además, se puede afirmar que todos los países participantes se encuentran en condiciones de obtener la equivalencia técnica para obtener la certificación de la Unión Europea y de esta forma poder avanzar en nuevas interoperabilidades dentro de la región con la inclusión del IPS.

## Lecciones Aprendidas

La realización de la Conectaton LACPASS fue el primer evento en América Latina y el Caribe el cual tenía como objetivo realizar pruebas de intercambio de información entre los países participantes. Generando un precedente y un punto de partida para continuar con el trabajo en conjunto entre todos los países de la región para lograr a futuro poder realizar el intercambio de información clínica transfronterizo, así como la inclusión del IPS.

A continuación, realizaremos la descripción sobre las lecciones aprendidas obtenidas de la Conectaton LACPASS:

- Creación de un ámbito colaborativo de intercambio de información y experiencias que le permitió a los países participantes poder adquirir conocimiento desde las experiencias de otros, así como poder evacuar dudas.
- La importancia de brindar a los participantes desde lo previo a la realización de la Conectaton LACPASS información técnica de calidad, en lo que contribuye a que los participantes tengan la información clara, lo que permite crear una base sólida de conocimiento.
- La realización de cursos de preparación previos, así como charlas con expertos en temas relacionados a la Conectaton como son IHE, IPS, entre otros
- Es muy importante que este tipo de evento el que tiene por objetivo realizar pruebas de intercambio de información clínica que cuenten con un alto grado de conectividad que permita realizar las actividades sin inconvenientes.
- Contar con un equipo de apoyo técnico presente en todo el desarrollo del evento ya que permite no solo solucionar imprevistos que puedan surgir sino también contribuir con los participantes a que puedan cumplir con los objetivos planteados.

# Anexos

## Anexo 1- Documentación Técnica LACPASS

Este documento se presenta como documentación técnica para la implementación de LACPASS, en el cual se detalla cómo opera la solución y los pasos necesarios que deben hacer los países participantes para integrarse a LACPASS.

El Pase de Vacunación de Latinoamérica y el Caribe, LACPASS, es una aplicación de intercambio de información sobre estados de vacunación de los países de América Latina y el Caribe, que permite que personas que hubiesen recibido parte o la totalidad del esquema de vacunación COVID en su país de residencia, al momento de viajar a otro país de la región puedan validar de forma simple y verificable su estado de vacunación en el país de destino, sin necesidad de realizar trámites adicionales como la homologación del certificado local de vacunación.

El proyecto LACPASS es una iniciativa de Red Americana de Cooperación en Salud Electrónica de América Latina y el Caribe (RACSEL), patrocinada por el Banco Interamericano de Desarrollo (BID) y ejecutada por el Centro Nacional de Sistemas de Información de Chile (CENS) por medio de la empresa privada Create de Chile, la cual se adjudicó la licitación para el desarrollo y puesta en marcha de este bien público.

La tecnología detrás de LACPASS se basa en el Digital Green Certificates de la Unión Europea (EU-DGC), este repositorio es un proyecto de código abierto usado en todos los países de la Unión Europea y 24 países fuera de ella. Este pase es multilingüe y está disponible en inglés, Español, Francés y Portugués los cuales son de especial interés en esta región. Además, permite ser digital y en papel, y posee un código QR verificable a través de las aplicaciones que provee el DGC. Al conectar a los países interesados a LACPASS es posible usar la misma tecnología para conectarse al Digital Green Certificates de la Unión Europea.

El principal objetivo del proyecto LACPASS es conectar de forma segura y verificable la información sobre vacunación individual de los residentes de los países de la región en un sistema uniforme e interoperable que facilite los viajes dentro de la región entregando a las autoridades sanitarias y migratorias de los países una herramienta que le entregue información veraz y oportuna sobre el estado de vacunación de los pasajeros que se encuentran entrando o transitando.

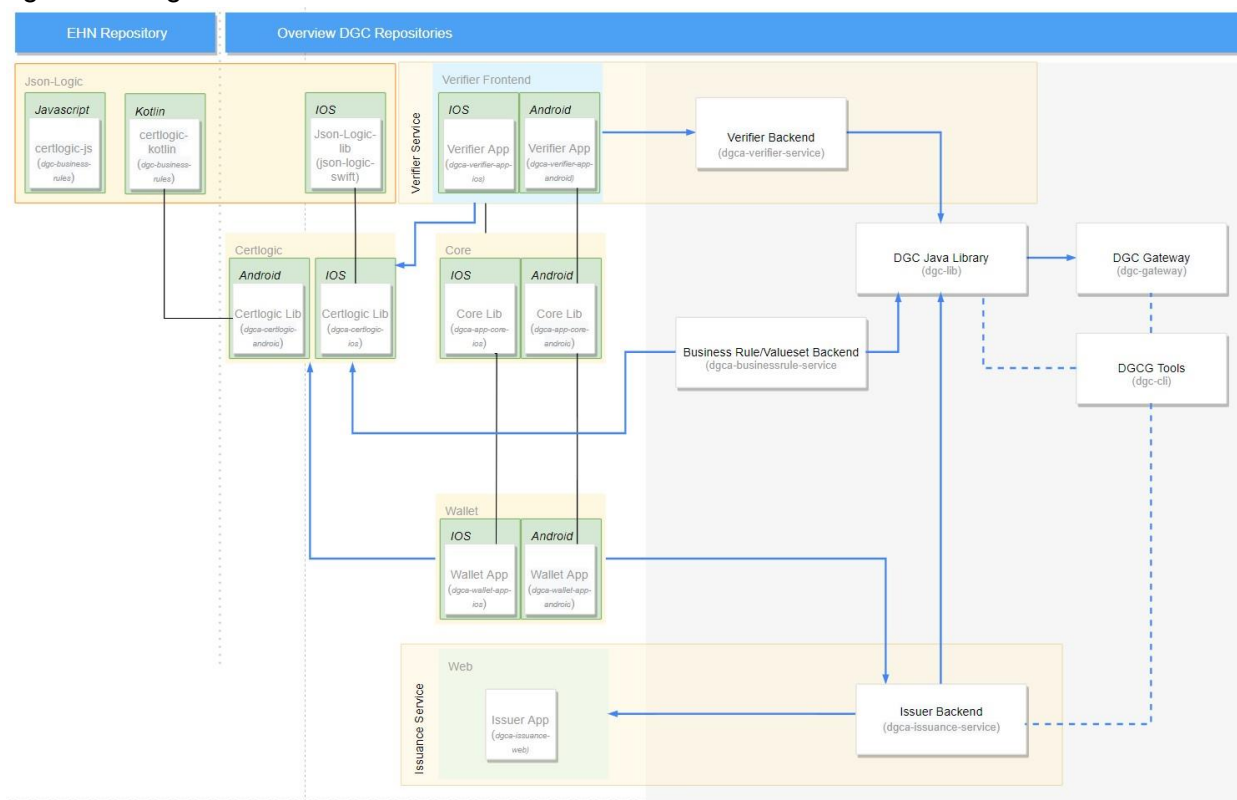
Como objetivo adicional, se busca colaborar con los países de la región para que puedan conectarse de forma simple y fluida a la tecnología del Digital Green Certificates de la Unión Europea.

## Arquitectura

Como se explicó anteriormente la implementación de LACPASS se basa en los proyectos de Digital Green Certificates de la Unión Europea (DGC) y European Health Network (EHN), cuyos repositorios se encuentran en los siguientes enlaces:

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

La DGC provee distintos repositorios para la implementación de interoperabilidad de certificados de vacunación. La interacción de todos estos repositorios está mostrada en el siguiente diagrama.



Funcionalmente los repositorios se pueden dividir en 3 grupos:

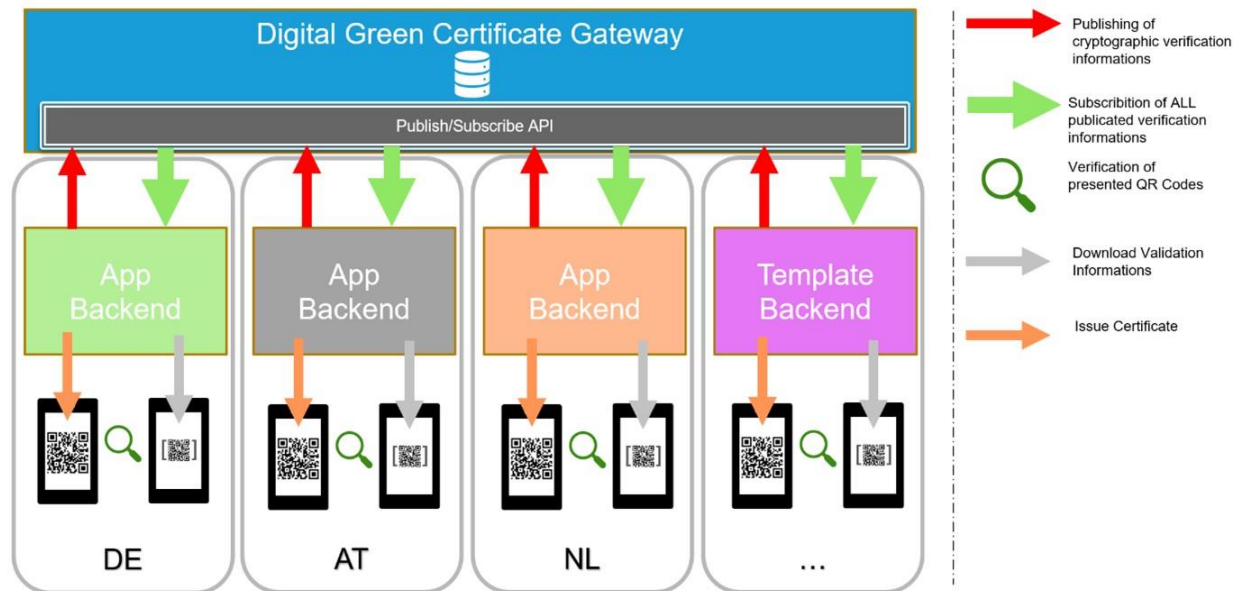
## Lógica y Sincronización

### Gateway

El DGC Gateway tiene el propósito de servir de soporte para todo el sistema DGC, provee todos los servicios necesarios para el traspaso seguro de validaciones y verificaciones entre sistemas nacionales. Cada sistema nacional puede implementar su propio DGC Gateway para obtener la libertad de distribuir las llaves con la tecnología preferida y además para poder manejar sistemas de verificación nacionales.

Adicionalmente si el certificado es generado en un formato estándar correcto, cualquier dispositivo verificador podrá verificar códigos de cualquier país que tenga el formato EU. Esto funciona tanto para el verificador conectado al sistema nacional como los sistemas offline que tengan descargadas las llaves públicas necesarias de antemano.

En el siguiente diagrama se muestra el flujo entre los distintos sistemas nacionales y el DGC Gateway:



Aquí hay un enlace con documentación detallada del DGC Gateway ([Documentación](#))

### [Business Rule Service](#)

El DGC Business Rule Service es uno de los servicios conectados al DGC Gateway, este servicio provee de las reglas necesarias para poder verificar si un código es o no válido en un sistema nacional. Estas reglas están basadas en las vacunas que posee, los test realizados y el estado de recuperación de la persona validada.

Para generar estas reglas de validación existe un formato más detallado en este enlace ([Business Rules Test Data](#)).

### Emisión

#### [Issuance Service](#)

El DGC Issuance Service es el sistema backend que provee los servicios tanto de creación como de firma de nuevos certificados (green certificates). Cada país debe levantar este servicio para poder tener los certificados. Para que los certificados puedan ser usados internacionalmente se deben compartir las llaves públicas en el Gateway para que todos los

países puedan verificar los certificados. Este servicio es usado por las aplicaciones móviles (Android, iOS) y por la aplicación web.

## Issuance Web

El Issuance Web es una aplicación web que provee una interfaz de usuario usada para proveer los datos necesarios en el issuance service. También se pueden generar certificados en esta aplicación.

## Verificación

### Verifier Service

Para verificar los certificados es necesario tener las llaves públicas del sistema nacional adecuado. El DGC Verifier Service es un servicio backend que se utiliza para gestionar las llaves públicas obtenidas a través del DGCG. Este servicio se utiliza en las aplicaciones móviles para obtener las llaves públicas y verificar los green certificates.

Para verificar los certificados se puede usar tanto el verificador en [iOS](#) como en [Android](#). Ambos repositorios contienen una aplicación muy simple para escanear los códigos QR y una interfaz de verificación y validación de estos.

## Seguridad y Llaves de Encriptación

El sistema del DGC usa un sistema de seguridad basado en el paradigma de llaves públicas y privadas que se usan para verificar la autenticidad de las consultas y la firma de los certificados. Algo importante de notar es que estas llaves públicas son verificadas directamente por la aplicación del DGC y no necesariamente siguen las reglas usuales de HTTPS.

Dentro de los repositorios se usan distintos formatos y estándares para el guardado de las llaves, a continuación se describe cada uno de estos formatos:

- **PEM:** Archivo que contiene una llave pública y opcionalmente una llave privada de forma plana. Generalmente sólo se incluye la llave pública.
- **KEY:** Archivo que contiene una llave privada de forma plana. Este archivo **nunca debería ser compartido** con terceros para evitar ataques y vulnerabilidades.
- **P12:** Archivo que contiene una llave pública y opcionalmente una privada de forma encriptada por una contraseña. Normalmente se toma como entrada un archivo PEM para construir un P12.
- **JKS:** Formato similar al P12 que es capaz de ser leído por aplicaciones Java de forma simple.

# Implementación

Esta sección describe los pasos que son necesarios realizar para que un nuevo país participante se incluya en LACPASS.

## Tecnologías

Los repositorios del “*EU Digital Covid Certificates*” (EUDCC) proveen APIs que están desarrollados en Spring Framework usando Java como lenguaje de programación primario. Las bases de datos utilizadas son Mysql y Postgresql. La aplicación web de emisión de certificados está desarrollada en React. Y las aplicaciones móviles están desarrolladas de forma nativa en Kotlin (Android) y Swift (iOS). Todos los proyectos a excepción de las aplicaciones móviles están disponibles a través de Docker.

## Requisitos del Servidor

Se requiere de un servidor el cual alojará los repositorios de los servicios web. Las características de este servidor dependerán del tráfico estimado, pero se recomienda un servidor con al menos 4 vCPU, 8 Gb de RAM y 50 Gb de disco.

El servidor también alojará las llaves de encriptación necesarias para el funcionamiento de las aplicaciones, por esto se recomienda que también cuente con un Hardware security module (HSM) para el manejo de estas llaves.

## Pre-requisitos

A continuación se darán los pasos a seguir para levantar cada uno de los repositorios del EUDCC. Pre-requisitos:

- OpenJDK 11
- Maven
- Autenticarse con [Github Packages](#)
- Docker (opcional)
- Docker-compsoe (opcional)
- Node 14
- OpenSSL
- [DGC-CLI](#)

Para poder instalar las dependencias a través de Maven en los repositorios que utilizan Spring como tecnología, se necesita estar autenticado por Github. Para esto se necesita crear un [token de acceso personal](#), que tenga la opción “*read:packages*” seleccionada. Luego se debe rellenar el archivo de configuración de maven (en linux ubicado en `~/.m2/settings.xml`) como el que se muestra a continuación:

```
<?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

El gateway es utilizado para compartir y verificar información a través de todos los países conectados a él. Por lo que no deberá ser incluido en el backend de cada país, acá se explica cómo levantar un gateway solo con el fin de poder probar la conexión de otros servicios. El repositorio puede ser clonado utilizando:

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

## Llaves

Para correrlo de manera local se necesita crear un *TrustAnchor*. El *TrustAnchor* es usado para firmar entradas en la base de datos. Para crear el *TrustAnchor* se usa el siguiente comando:

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

Luego la llave pública se exporta al Keystore de Java utilizando:

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

Donde “cert\_ta.pem” es la llave pública y “dgcg-p4ssw0rd” es la clave de la llave. Esta llave “ta.jks” debe ser colocada en una carpeta nombrada “certs”, la cual debe ser creada en la raíz del repositorio.

## Base de datos

Este repositorio utiliza una base de datos MySQL, si es que no se utiliza docker para construir el proyecto, se necesita instalar y crear una base en MySQL.

### Configuración

Para configurar variables como por ejemplo el directorio de la llave pública y la conexión a la base de datos, se puede hacer de dos maneras. Si es que se utiliza Docker para ejecutar el proyecto se pueden editar las variables de entorno que se muestran en “docker-compose.yml”, para más detalles sobre este archivo la documentación está disponible en el siguiente [link](#). Si es que no se utiliza docker se puede editar el archivo de configuración de Spring en

“~/dgc-gateway/src/main/resources/application.yml”

### Ejecutar

Para construir el ejecutable del proyecto, el cual es construido a través de Maven, se utiliza el siguiente comando:

```
$ mvn clean install
```

Si es que se utilizara docker para correr el proyecto se le debe agregar una bandera extra al comando anterior:

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

Esto creará un archivo “jar” en el directorio “~/dgc-gateway/target”. Para correr la aplicación se utiliza:

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

Y si se utiliza Docker, se puede utilizar:

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

Lo cual subirá la API del gateway junto con una base de datos mysql. Para poder hacer consultas a la API de este gateway, es necesario registrar ciertos certificados que pertenecen al backend de cada país. Estos certificados serán de AUTHENTICATION, UPLOAD y CSCA. Para esto se pueden crear estos certificados con 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
```

Estos certificados deben ser firmados por el *TrustAnchor* del gateway (“cert\_ta.pem” y “key\_ta.pem”), para esto se puede usar el cliente facilitado por el EUDCC. Este se puede bajar en este [link](#). Luego usando este jar, se pueden ejecutar los siguientes comandos:

```
$ 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
```

En cada uno de estos comandos se entregara un “TrustAnchor Signature”, “Certificate Raw Data”, “Certificate Thumbprint” y “Certificate Country”. Estos valores tienen que ser ingresados en la tabla “trusted\_party” de la base de datos del gateway, por lo que se agregaran tres nuevas líneas en esta tabla (por cada uno de los certificados). Esto puede hacerse usando:

```
$ 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;
```

Para probar que los valores fueron ingresados correctamente, se le puede hacer una petición a la API del gateway utilizando el thumbprint de autenticación:

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

Lo cual deberá entregar la lista de certificados en la tabla “trusted\_parties”.

## [Business rule](#)

Este repositorio contiene un backend con las reglas de negocio para aceptar/rechazar los estados de los certificados COVID emitidos por los países. El repositorio puede ser clonado utilizando:

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

### LLaves

Este repositorio necesita tres llaves, un trust\_anchor, trust\_store y key\_store. El trust\_anchor es el TrustAnchor creado en el gateway, el trust\_store puede ser creado utilizando el certificado y llave de autenticación que fueron registradas en el gateway de la siguiente manera :

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

El truststore es creado utilizando el certificado de autenticacion, con el comando:

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

### Base de datos

Este repositorio utiliza una base de datos Postgresql, si es que no se utiliza docker para construir el proyecto, se necesita instalar y crear una base en Postgresql.

### Configuración

Para configurar variables como por ejemplo el directorio de las llaves y la conexión a la base de datos, se puede hacer de dos maneras. Si es que se utiliza Docker para correr el proyecto se pueden editar las variables de entorno que se muestran en “docker-compose.yml”, para más detalles sobre este archivo la documentación está disponible en el siguiente [link](#). Si es que no se utiliza docker se puede editar el archivo de configuración de Spring en

“~/dgc-gateway/src/main/resources/application.yml”. Las variables mas importantes se muestran a continuación:

```
# 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>
```

### Ejecutar

Para construir el ejecutable del proyecto, el cual es construido a través de Maven, se utiliza el siguiente comando:

```
$ mvn clean install
```

Esto creará un archivo “jar” en el directorio “~/dgc-businessrule-service/target”. Para correr la aplicación se utiliza:

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

Y si se utiliza Docker, se puede utilizar:

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

### Reglas

En esta sección se explica brevemente cómo generar un archivo JSON con las reglas de validación de los certificados. Estas reglas determinan si una persona que entra a un país es considerada apta para entrar a este país, las reglas se basan en las vacunas administradas, los test que ha realizado y el estado de recuperación después de contraer COVID. Todas estas reglas deben estar codificadas según los estándares del Digital COVID Certificate. Para generar las reglas de validación se requiere generar un json con lo siguiente:

- Cumplir la semántica [CertLogic](#)
- Tener el esquema estándar ([Schema](#))
- Los campos especificados en “AffectedFields” deben estar contenidos en el esquema DCC. ([DCC Schema](#))

CertLogic es una semántica que extiende la semántica [JsonLogic](#). Estas semánticas usan reglas intuitivas y simples para poder verificar patrones o lógicas dentro de un archivo Json. Usan operadores lógicos como la igualdad (“==”), operadores numéricos, etc. Estos operadores puedes encontrarlos [aquí](#).

Aquí se muestra un ejemplo de cómo se construye un Json con la semántica CertLogic:

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

Ahora para generar un archivo con los [estándares](#) correctos se debe seguir el esquema correctamente, para esto se deben agregar los siguientes campos:

- **AffectedFields:** Arreglo de reglas que se usarán del payload (QR).
- **Country:** Código ISO del país. (Ej: "CL").
- **CertificateType:** Tipo del certificado. Los valores válidos son "General", "Test", "Vaccination", "Recovery". Si por ejemplo la regla busca el tiempo mínimo después de un test de COVID este certificado es del tipo "Recovery".
- **Description:** Arreglo con la descripción de la regla, aquí se agregan todos los idiomas que se quiera soportar.
- **Engine:** Tipo de semántica usada. (Ej: "CERTLOGIC")
- **EngineVersion:** Versión de la semántica. Actualmente es la "1.2.2".
- **Identifier:** Identificador único de la regla. Debe ser el patron `^\{GR|VR|TR|RR|IR\}-[A-Z]{2}-\d{4}$`. Por ejemplo si la regla es de "Recovery", el país es Chile y además es la primera regla, el identificador es "RR-CL-0000".
- **Logic:** Objeto donde se establece la regla. Aquí se usa la semántica para definir la regla.
- **SchemaVersion:** Versión del esquema usado.
- **Type:** Tipo de la regla, puede ser de aceptación ("Acceptance") o invalidación ("Invalidation").
- **ValidFrom:** Hasta que fecha esta regla es válida (sin ms y con zona horaria).
- **ValidTo:** Desde que fecha esta regla es válida (sin ms y con zona horaria).
- **Version:** Versión de la regla.

Para entender mejor cómo se genera este archivo se explicara de forma general cómo construir los campos "Logic" y "AffectedFields". Para el campo "AffectedFields" se debe entender como llega el payload (contenido del QR), el contenido tiene un formato estándar que se puede encontrar en este [enlace](#). El objeto payload debe contener al menos uno de los siguientes campos:

- “v”: Contiene todo lo relacionado con la vacunación (“Vaccination Entry”).
- “t”: Contiene todo lo relacionado con los tests realizados (“Test Entry”).
- “r”: Contiene todo lo relacionado con la recuperación (“Recovery Entry”).

Cada uno de estos campos puede contener atributos específicos a lo que representa, detallaremos en los siguientes puntos que puede contener cada uno.

## Vaccination Entry (“v”)

- tg: Enfermedad o agente objetivo.
- vp: Vacuna o profilaxis.
- mp: Medicamento de la vacuna.
- ma: Empresa de marketing autorizada o fabricante.
- dn: Número de la Dosis.
- sd: Total de dosis (Serie de dosis, por ejemplo serían 2 si se requieren dos dosis).
- dt: Fecha de vacunación. ● co: País de vacunación.
- is: Emisor del certificado.
- ci: Identificador único del certificado (UVCI).

## Test Entry (“t”)

- tg: Enfermedad o agente objetivo.
- tt: Tipo de test.
- nm: Prueba de ácido nucleico.
- ma: Nombre de la prueba rápida de antígenos y fabricante.
- sc: Fecha/Hora de recolección de la muestra.
- tr: Resultado del examen.
- tc: Centro encargado del examen.
- co: País del examen.
- is: Emisor del certificado.
- ci: Identificador único del certificado (UVCI).

## Recovery Entry (“r”)

- tg: Enfermedad o agente objetivo.
- fr: Fecha primer positivo del test de ácido nucleico.
- co: País del examen.
- is: Emisor del certificado.
- df: Fecha desde que el examen es válido.
- du: Fecha hasta cuando es válido el examen. ● ci: Identificador único del certificado (UVCI).

Existe un documento oficial sobre la documentación de este estándar, en este [enlace](#).

Para entender mejor cómo se eligen los valores, tomaremos como ejemplo la regla “La serie de vacunación debe estar completa (por ejemplo, 1/1, 2/2)”. Para este ejemplo los valores de “AffectedFields” serían los siguientes:

```
"AffectedFields": [  
  "v.0", // Se necesitan los valores de vacunación.  
  "v.0.dn", // Dosis actual.  
  "v.0.sd" // Número de dosis total de la serie.  
]
```

Ya entendiendo cómo se arma el “AffectedFields” siguiendo con el mismo ejemplo vamos a construir la lógica de la regla: “La pauta de vacunación debe estar completa (por ejemplo, 1/1, 2/2)”. Lo primero que hay que notar es que es una regla de vacunación entonces se usa la parte “v” del payload. Además como se busca comprobar las series de vacunación se usará tanto “dn” y “sd” donde sacaremos la información de la dosis actual y el total de dosis requeridos respectivamente. Entonces para validar el esquema de vacunación completo se debe verificar que ambos valores sean los mismos, como se muestra en en el siguiente esquema:

```
"Logic": {  
  "if": [ // Si es que se cumple lo contenido, se acepta la regla.  
    {  
      "var": "payload.v.0" // Se explicita de donde obtener los valores.  
    },  
    {  
      "===": [ // Se usa el operador de igualdad exacta.  
        {  
          "var": "payload.v.0.dn" // Actual Dosis (Número en la serie).  
        },  
        {  
          "var": "payload.v.0.sd" // Número de dosis total de la serie.  
        }  
      ]  
    }  
  ]  
}
```

Este ejemplo fue extraído de las reglas de España [aquí](#). Si necesitas más ejemplos puedes ver los recomendados por la EU ([Más ejemplos](#)).

## Issuance

Este repositorio contiene un backend con que permite la emisión de certificados de vacunación. El repositorio puede ser clonado utilizando el siguiente comando:

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

## LLaves

Este proyecto no requiere crear nuevas llaves, se utilizarán las mismas creadas anteriormente para el business rule. De hecho en vez de copiar las llaves entre los repositorios se recomienda tener un directorio en donde todos los repositorios compartan las llaves y se compartan a través de link simbólicos o volúmenes de docker.

## Base de datos

Este repositorio utiliza una base de datos Postgresql, si es que no se utiliza docker para construir el proyecto, se necesita instalar y crear una base en Postgresql.

## Configuración

Al igual que el business rule, la configuración del repositorio se encuentra en el archivo docker-compose.yml, pero también se puede cambiar directamente el archivo "src/main/resources/application.yml" en caso de no utilizar docker.

El servicio de issuance tiene dos formas de ejecución: una de testing y otra conectada a un gateway. Ambas se explican a continuación:

**Configuración de Testing:** Esta es la que viene por defecto y sirve para probar rápidamente la emisión de certificados sin tener que instalar un gateway. No se requiere mayor configuración para operar en este modo y se utiliza una llave de prueba genérica para la firma de los certificados.

**Configuración Producción:** Esta configuración se conecta a un gateway y permite interoperar con los demás servicios del DGC. Para acceder a esta configuración hay que cambiar el docker-compose.yml y agregar las siguientes configuraciones al backend

backend:

environment:

```
... # MANTENER LO QUE ESTA Y AGREGAR LO SIGUIENTE
# 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
```

Asegurarse de reemplazar correctamente las llaves. Más información de esta configuración en [este link](#).

### Ejecutar

Para construir el ejecutable del proyecto, el cual es construido a través de Maven, se utiliza el siguiente comando:

```
$ mvn clean package
```

Esto creará un archivo “jar” en el directorio “~/dgc-issuance-service/target”. Para correr la aplicación se utiliza:

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

Y si se utiliza Docker, se puede utilizar:

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

Al finalizar, en el puerto indicado en la configuración se debería levantar el servicio web que emite certificados. Por ejemplo si se usa el puerto 8081 se puede navegar a esta URL:

<http://localhost:8081/swagger>

### Cliente Web

Para probar la emisión de certificados, la DGC provee otro repositorio llamado [issuance-web](#). Este corresponde a una aplicación web que consume la API entregada por el issuance-service y permite generar certificados de vacunación. Esta aplicación funciona independiente si se eligió el modo de Testing o modo productivo en el issuance-service. Para clonar el repositorio se puede ejecutar el siguiente comando:

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

Luego para conectar con las APIs es necesario modificar el archivo docker-compose.yml, o bien cambiar el archivo de configuración de nginx.

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

Aquí se debe especificar las URLs del issuance-service y business rule. Algo importante a notar es que este repositorio trae como dependencias estos dos servicios, dado que en esta guía estamos levantando y configurando cada servicio por separado es necesario eliminar estos de la configuración.

Finalmente se puede ejecutar la aplicación web usando el siguiente comando

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

## Verifier

Este repositorio contiene un backend con que permite la verificación de certificados emitidos de vacunación. El repositorio puede ser clonado utilizando el siguiente comando:

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

## LLaves

Al igual que el issuance service este repositorio necesita las llaves previamente creadas.

## Base de datos

Este repositorio utiliza una base de datos Postgresql, si es que no se utiliza docker para construir el proyecto, se necesita instalar y crear una base en Postgresql.

## Configuración

Al igual que el issuance-service, la configuración del repositorio se encuentra en el archivo docker-compose.yml, pero también se puede cambiar directamente el archivo "src/main/resources/application.yml" en caso de no utilizar docker.

Para el verifier-service no existe un modo de testing, por lo que siempre se utiliza con un gateway asociado. Para configurarlo es necesario modificar el archivo de configuración e indicar las rutas al gateway y a las llaves:

```
- 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
```

## Ejecutar

Al igual que los repositorios anteriores, para construir el ejecutable del proyecto, se utiliza el siguiente comando de Maven:

```
$ mvn clean install
```

Esto creará un archivo “jar” en el directorio “~/dgc-verifier-service/target”. Para correr la aplicación se utiliza:

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

Y si se utiliza Docker, se puede utilizar:

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

Al finalizar, en el puerto indicado en la configuración se debería levantar el servicio web que emite certificados. Por ejemplo si se usa el puerto 8082 se puede navegar a esta URL:

<http://localhost:8082/swagger>

## Aplicaciones Móviles de Verificación

Para las aplicaciones móviles los repositorios se dividen en las plataformas iOS y Android. Ambas plataformas tienen 4 repositorios divididos por funcionalidades que cumplen cada uno. Para los desarrollos de levantamiento de aplicaciones para verificar los certificados solo se modificarán los repositorios “verifier” y “wallet” según lo que se necesite. Los repositorios de ambas plataformas son las siguientes:

- **App Core:** Este repositorio contiene todos los servicios necesarios para conectarse al DGC Verifier Service y con el DGC Business Rule. También se encarga de firmar los certificados para poder enviarlos de forma segura.
  - 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:** Este repositorio contiene la aplicación móvil que se encarga de escanear y verificar los certificados usando las llaves públicas, usa el App Core para hacer los llamados pertinentes.
  - 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:** Este repositorio provee una interfaz de usuario para poder administrar y guardar los DGCs personales.
  - 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:** Este repositorio contiene el código fuente para poder manejar la semántica CertLogic en las aplicaciones móviles.
  - iOS: <https://github.com/eu-digital-green-certificates/dgc-certlogic-ios>

- Android: <https://github.com/eu-digital-green-certificates/dgc-certlogic-android>

En caso de que se requiera ejemplos de códigos QR, están estos ejemplos oficiales (<https://dgc.a-sit.at/ehn/testsuite>).

## IOS

Los requisitos para los servicios en iOS son:

- Se necesita un Mac o una máquina virtual para correr Xcode.
- Xcode 12.5+ es usada para las compilaciones. Se requiere un sistema operativo macOS 11.0+.
- Para instalarlo en dispositivos físicos, se necesita una cuenta de desarrollador de Apple.  
Para esto debes enrollar en el programa de desarrollo de apple ([Apple Developer Program](#))

## Verifier

Este repositorio contiene la aplicación móvil para verificar certificados a través de iOS. Para poder instalar este proyecto primero debes clonarlo localmente con el siguiente comando:

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

Para poder tener los servicios de conexión y firma de certificados debes tener además el repositorio core en la misma carpeta, puedes usar el mismo comando usado para clonar el repositorio core.

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

Una vez que tengas instalados ambos repositorios, deben modificar el archivo context.jsonc con los valores correctos del sistema nacional. Este archivo se encuentra en la carpeta "context". Debes rellenar los valores adecuados como se muestra en el siguiente esquema:



Para poder tener los servicios de conexión y firma de certificados debes tener además el repositorio core en la misma carpeta, puedes usar el mismo comando usado para clonar el repositorio core.

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

Al igual que el verifier debes modificar el context.jsonc para poder generar el certificado personal. También se puede modificar la localización en el mismo archivo.

## Android

Los requisitos para los servicios en Android son:

- Para el desarrollo se recomienda usar Android Studio. La última versión disponible se puede descargar [aquí](#).
- Android SDK version 26+

### Verifier y Wallet (Android)

Este repositorio contiene la aplicación móvil para verificar certificados a través de Android. Para poder instalar este proyecto primero debes clonarlo localmente con el siguiente comando:

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

Para poder tener los servicios de conexión y firma de certificados debes tener además el repositorio core en la misma carpeta, puedes usar el mismo comando usado para clonar el repositorio core.

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

Una vez que tengas instalados los repositorios, deben modificar el archivo verifier-context.jsonc con los valores correctos del sistema nacional. Este archivo se encuentra en la carpeta "app/src/acc/assets". Debes generar un archivo llamado "config.json" en la misma carpeta y rellenar los valores adecuados como se muestra en el siguiente esquema:

## 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



## Preguntas Frecuentes

Esta sección describe las preguntas más frecuentes relacionadas al proyecto

- Si estoy usando el issuance-web, ¿cómo se puede agregar autenticación o alguna medida de restricción de acceso?

La aplicación web de issuance (issuance-web) no cuenta con un sistema de autenticación propio ni ninguna medida de control de acceso. Esto quiere decir que una vez desplegada esta aplicación cualquier usuario que tenga acceso al servidor puede usarla y emitir certificados. Existen distintas estrategias para controlar el acceso dependiendo de la complejidad y cantidad de recursos que posean los países.

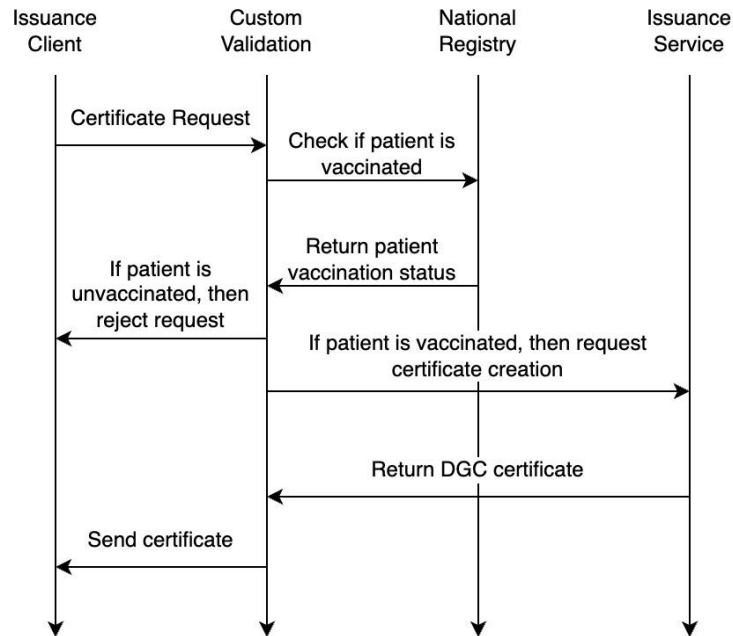
La alternativa más simple de implementar es agregar autenticación HTTP básica al servidor de proxy ya sea nginx o apache. Ambos proveen plugins para agregar este tipo de autenticación, por ejemplo configurando el archivo `.htpasswd`.

La siguiente opción recomendada es no utilizar el servicio de issuance-web y desarrollar una aplicación propia que utilice la API del issuance-service. De esta forma se tiene control total del desarrollo y se puede agregar autenticación a nivel de la aplicación.

De todas formas se recomienda que la aplicación esté sólo visible para un segmento específico de IPs o ubicaciones para evitar otro tipo de tráfico.

- Si tengo un registro nacional de personas vacunadas, ¿cómo puedo integrar esta información al sistema?

Los países con un Registro Local de Vacunación pueden conectar la información de las personas vacunadas a LCPASS por medio de la API del issuance-service. Lo recomendado es crear un software que se inserte entre el cliente de emisión de certificados (issuance-web o desarrollo propio) y el issuance-service. Este software debería verificar la autenticidad del certificado solicitado a emitir con el registro nacional y continuar con el proceso de emisión o detenerlo en caso que los datos solicitados no coincidan. El siguiente diagrama ejemplifica el funcionamiento.



- ¿Cuáles son los pasos a seguir para poder integrarse con la UE?

El proceso de integración está explicado en el siguiente enlace: [Onboarding Checklist](#).

A modo general el proceso consiste en enviar a la UE las llaves públicas para agregarlas a la base de datos del gateway tal como se explicó en la sección del gateway. Y luego de hacer pruebas de que todo esté funcionando correctamente, se necesita cambiar el endpoint del gateway al endpoint oficial de ellos.

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.

- ¿Cómo manejar las personas que se vacunan por primera vez y las personas que ya se encuentran vacunadas?

Es recomendable que los países que tienen implementado un Registro Local de Vacunación lo hayan integrado usando las instrucciones anteriores. De esta forma, la capa de validación propia que se debe desarrollar puede manejar los casos en los cuales las personas ya estuvieron vacunadas o se han vacunado por primera vez o tienen su esquema de vacunación incompleto.

## Anexo 2- Casos de Prueba Conectaton LACPASS

### Casos de Prueba

#### 1.1 Objetivo General:

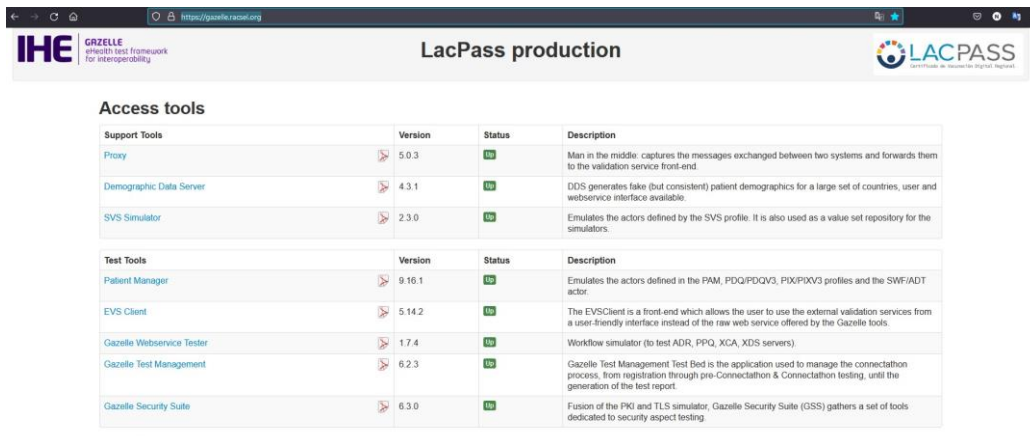
Desarrollar actividades técnicas que permitan demostrar que es actualmente viable que los diferentes sistemas de información de los países accedan, intercambien, integren y utilicen de manera cooperativa los datos asociados a los certificados COVID-19, mediante el uso e interacción con los servicios del directorio regional de LACPass -el cual está basado en la definición EU DCC- y la plataforma de pruebas Gazelle de IHE.

#### 1.2 Objetivos específicos:

1. Crear y emitir certificados digitales COVID-19 según estándar EU-DCC.
2. Validar los certificados emitidos dentro del mismo país con la plataforma Gazelle.
3. Verificar entre pares certificados COVID-19 emitidos por los participantes.

#### 1.3 Metodología:

1. Generación de certificados según EU-DCC desde cada plataforma local. Los datos para los casos de prueba por definición deben provenir de los mismos sistemas locales.
2. Utilización de la plataforma Gazelle para la validación y trazabilidad de los casos de prueba definidos. Plataforma Gazelle disponible en: <https://gazelle.racsel.org/> (figura 01).



The screenshot shows the IHE Gazelle LacPass production platform interface. The page title is "LacPass production". Below the title, there is a section titled "Access tools" which contains two tables. The first table lists "Support Tools" and the second table lists "Test Tools". Each table has columns for "Tool Name", "Version", "Status", and "Description".

Support Tools	Version	Status	Description
Proxy	5.0.3	OK	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	OK	DDS generates fake (but consistent) patient demographics for a large set of countries, user and webservice interface available.
SVS Simulator	2.3.0	OK	Emulates the actors defined by the SVS profile. It is also used as a value set repository for the simulators.

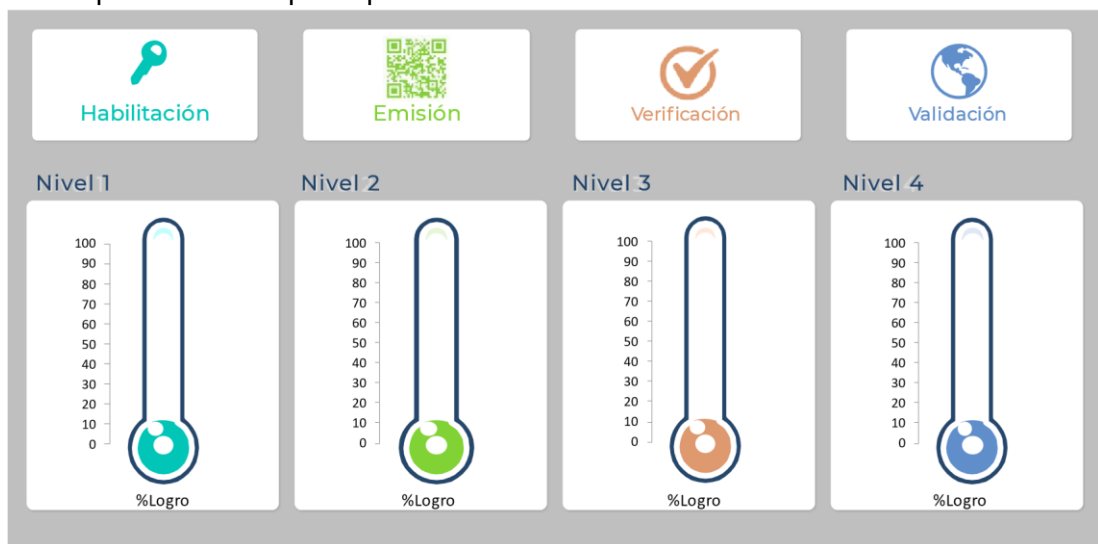
Test Tools	Version	Status	Description
Patient Manager	9.16.1	OK	Emulates the actors defined in the PAM, PDQ/PDQV3, PIX/PIXV3 profiles and the SWF/ADT actor.
EVS Client	5.14.2	OK	The EVSClient is a front-end which allows the user to use the external validation services from a user-friendly interface instead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

Fig.01: Plataforma de pruebas IHE Gazelle

3. La totalidad de los casos de prueba de la Conectaton LACPASS se encuentran disponibles y detallados en la plataforma Gazelle.
4. Se evaluarán cuatro niveles de cumplimiento para todos los participantes:

- a. **Nivel 1 - Habilitación:** Corresponde a la configuración correcta de los marcos de confianza, cargar y descargar de manera correcta las llaves públicas para la validación de los certificados COVID.
- b. **Nivel 2 - Emisión:** Corresponde a la correcta generación y emisión de los certificados COVID desde cada uno de los sistemas locales de los participantes.
- c. **Nivel 3 - Verificación:** Corresponde a la correcta verificación mediante la plataforma Gazelle, de los certificados COVID emitidos desde cada país
- d. **Nivel 4 - Validación:** Corresponde a la validación entre pares de los certificados COVID emitidos por cada país, este caso de prueba se repite n veces por cada participante que deba ser validado entre pares.

La figura 02 a continuación expone de manera grafica el monitoreo del cumplimiento de los niveles para todos los participantes de la Conectaton LACPASS.



**Fig.02: Niveles de cumplimiento asociados a los casos de test de la Conectaton LACPASS.**

#### 1.4 Lista casos de prueba Conectaton LACPASS:

La totalidad de los casos de test, su detalle y definición se encuentran disponibles en la plataforma Gazelle.

La tabla 01 siguiente detalla los casos de prueba a ejecutar con el link correspondiente a su descripción:

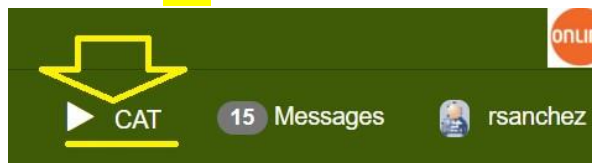
<b>Tests</b>	<b>Nombre de Test</b>	<b>Link a la descripción del Test</b>
Test 1	DCC - Recovery Certificate*	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=74">https://gazelle.racsel.org/gazelle/test.seam?id=74</a>
Test 2	DCC - Result Certificate*	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=76">https://gazelle.racsel.org/gazelle/test.seam?id=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	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 7	(Colombia)	
Test 8	DCC - Scan Digital Certificate	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 9	(Ecuador)	
Test 10	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 11	DCC - Scan Digital Certificate	<a href="https://gazelle.racsel.org/gazelle/test.seam?id=73">https://gazelle.racsel.org/gazelle/test.seam?id=73</a>
Test 12	(Paraguay)	
	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>
	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>
	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>

**Tabla 01: Listado de Casos de prueba.**

Los casos de prueba marcado con \* (Test 1 y 2) solo son requeridos para aquellos países que actualmente son capaces de emitir certificados de Test y Recuperado. Para los casos de validación de pares no aplica la verificación de su propio certificado (Test 5 al 12).

# Guía ejecución instancia de prueba

- **Paso 1:** Ve al menú **CAT**





- **Paso 2:** Busque la prueba que desea ejecutar y luego haga clic en el botón **+**

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				R / 7
	DCC - Validation Error Case				R / 1

- **Paso 3:** Seleccione el certificado de su país que desea probar haciendo clic en el botón **+**

## Start test instance

DCC - Scan Digital Certificate Configuration

Role	Systems	
	Organization Name	System keyword
 CERTIFICATE_CREATOR [1,1] ?		
0 Participants		
 CERTIFICATE_CONSUMER [1,1] ?		
	DHE	OTHER_DHE_MHD

Se mostrará la lista de certificados de países.

- **Paso 4:** Seleccione uno de ellos, luego haga clic en Agregar

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)

- **Paso 5:** Luego haga clic en el botón « **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

- **Paso 6:** Inicie una nueva instancia de prueba haciendo clic en el botón verde

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

OTHER\_MSP

⇒ Add all

→ Add

← Remove

⇐ Remove all


OTHER\_MINSAPERU\_COVID

Add selected partner(s)

- **Paso 7:** Ejecutar la instancia de prueba

## 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		
1 Participants						
✓ CERTIFICATE_CONSUMER [1,1] ?	DHE	OTHER_DHE_MHD	DCC	CERTIFICATE_CONSUMER		
1 Participants						



## Añadir enlace permanente en sus pruebas

Requisito previo: Validar un certificado en la herramienta Validador de códigos QR

- **Paso 1:** Valide su certificado y luego copie el enlace permanente

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
Validation service :	DCC Validator
Validation status :	<b>PASSED</b>
Permanent link :	<a href="https://gazelle.racsel.org/EVSCClient/qrCodeResult.seam?oid=1.3.6.1.4.1.12559.11.47.468">https://gazelle.racsel.org/EVSCClient/qrCodeResult.seam?oid=1.3.6.1.4.1.12559.11.47.468</a>
Validation date :	5/25/22 6:54:14 AM (BRT GMT-0300)
DGCG QR Code Status :	PASSED

- **Paso 2:** Vuelva a la instancia de prueba. En la parte inferior de la página, haga clic en el globo terráqueo para agregar el enlace permanente como prueba.

**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

