Universitat de les Illes Balears

Sistema de gestión de certificados digitales COVID-19 basado en Blockchain

Rosa Pericàs Gornals

Macià Mut Puigserver

M. Magdalena Payeras Capellà

Llorenç Huguet Rotger

Contenidos

1. Presentación del problema
2. Tecnologías utilizadas
3. Protocolo
4. Implementación
5. Conclusiones

Introducción

Certificado de Vacunación COVID

EU DIGITAL COVID CERTIFICATE
CERTIFICADO COVID DIGITAL DE LA UE
Vaccination · Vacunación

Surname and forename / Apellidos y nombre
[redacted]

Date of birth / Fecha de nacimiento
1989-10-28

Vaccination details / Datos de vacunación

Certificate identifier / Identificador del certificado
01ES05VAE2986783F23673589FAE#3

Certificate issuer / Emisor del certificado
Nombre del emisor

Disease targeted / Enfermedad que se previene	COVID-19
Vaccine/prophylaxis / Tipo de vacuna	SARS-CoV-2 mRNA vaccine / SARS-CoV-2 vacuna ARNm
Vaccine medicinal product / Vacuna administrada	COVID-19 Vaccine Moderna
Manufacturer / Fabricante	Moderna Biotech Spain S.L.
Number in a series of vaccinations and number of doses / Número en una serie de vacunaciones y número de dosis	1/2
Date of vaccination / Fecha de vacunación	2021-04-21
Member State of vaccination / Estado miembro de vacunación	ES

This certificate is not a travel document. The scientific evidence on COVID-19 vaccination, testing and recovery continues to evolve, also in view of new variants of concern of the virus. Before travelling, please check the applicable public health measures and related restrictions applied at the point of destination. / El presente certificado no es un documento de viaje. Los datos científicos sobre la vacunación, el test y la recuperación de la COVID-19 siguen evolucionando, también a la vista de las nuevas variantes preocupantes del virus. Antes de viajar, sírvase comprobar las medidas de salud pública aplicables y las restricciones correspondientes que se apliquen en el punto de destino.

Problemática asociada a los certificados de vacunación

El sistema de gestión debe **imposibilitar la falsificación** de certificados.

Característica que fue violada en diferentes países donde el uso se impuso como obligatorio.

Problemática asociada a los certificados de vacunación

euronews. My Europe World Business Sport Green Next Travel Culture Video Programmes

FRANCE

French authorities open 400 investigations into fake COVID-19 health passes

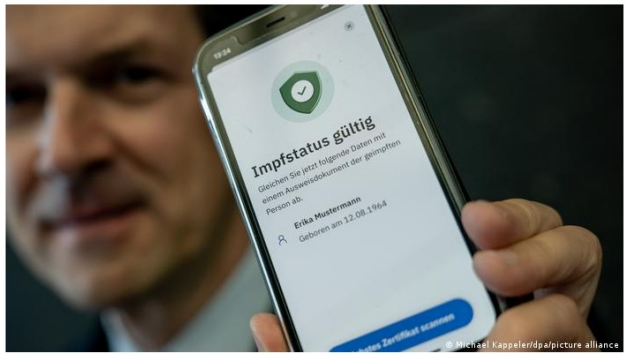
COMMENTS

By AP • Updated: 13/12/2021

NEWS

Germany sees increase in fake vaccination certificates

More than 2,500 cases of forged health documents have been reported to state police departments, with the majority created recently, according to a recent investigation by a German newspaper.



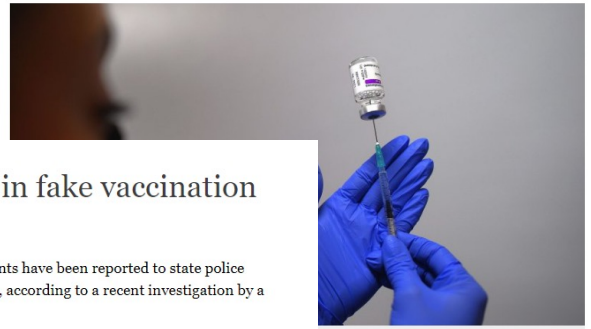
© Michael Kappeler/dpa/picture alliance

EURACTIV The Capitals The Brief Ukraine

Agrifood Digital & Media Economy & Jobs Energy & Environment Global Europe Health Politics Transport Brussels

Fake COVID passports flourish in southeastern Europe

By Krassen Nikolov and Zeljko Trkanjec | EURACTIV network 1 dic 2021



the side effects of COVID-19 vaccines. [EPA-EFE/VASSIL

Advertisement

EURACTIV Members

Acumen public affairs
BSEF - The International Bromine Council
Cosmetics Europe - The Personal Care Association
ECPC - European Cancer Patient Coalition

Medidas de seguridad en la generación de certificados

Restringir el número de personas que pueden generar dichos certificados

Añadir el uso de técnicas que garanticen la inmutabilidad de los datos.

Privacidad

Reglamento General de Protección de Datos de Europa (RGPD).

Los certificados contienen datos relativos a la **salud**.

Son considerados datos sensibles.

Requieren almacenamiento y compartición de forma segura y preservando la privacidad.

Requisitos de Seguridad

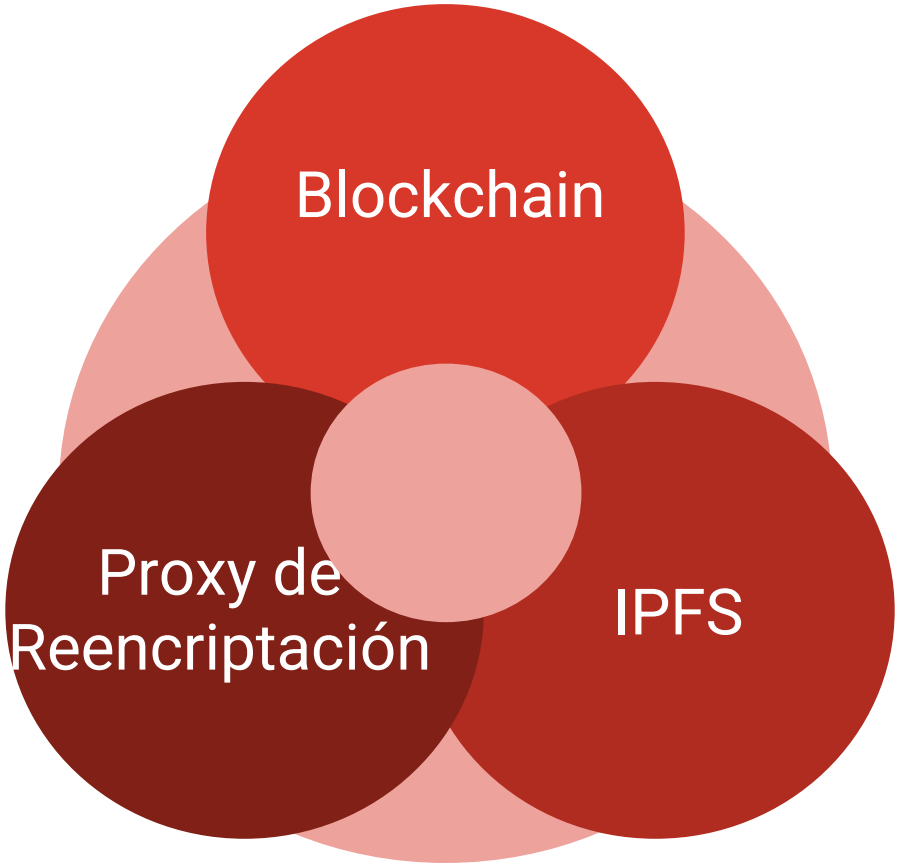
- Integridad
- Inmutabilidad
- Privacidad
- Confidencialidad
- Self - Sovereignty
- Autenticidad

Contribución

Supervisión de los emisores y verificadores.	Completo cifrado de los datos contenidos en los certificados.	Soberanía de los datos por parte del propietario.
Fácil verificación por entidades fiables.	Posibilidad de verificación por parte de entidades no fiables o usuarios.	Diseño del protocolo, Implementación y Test

Tecnologías Utilizadas

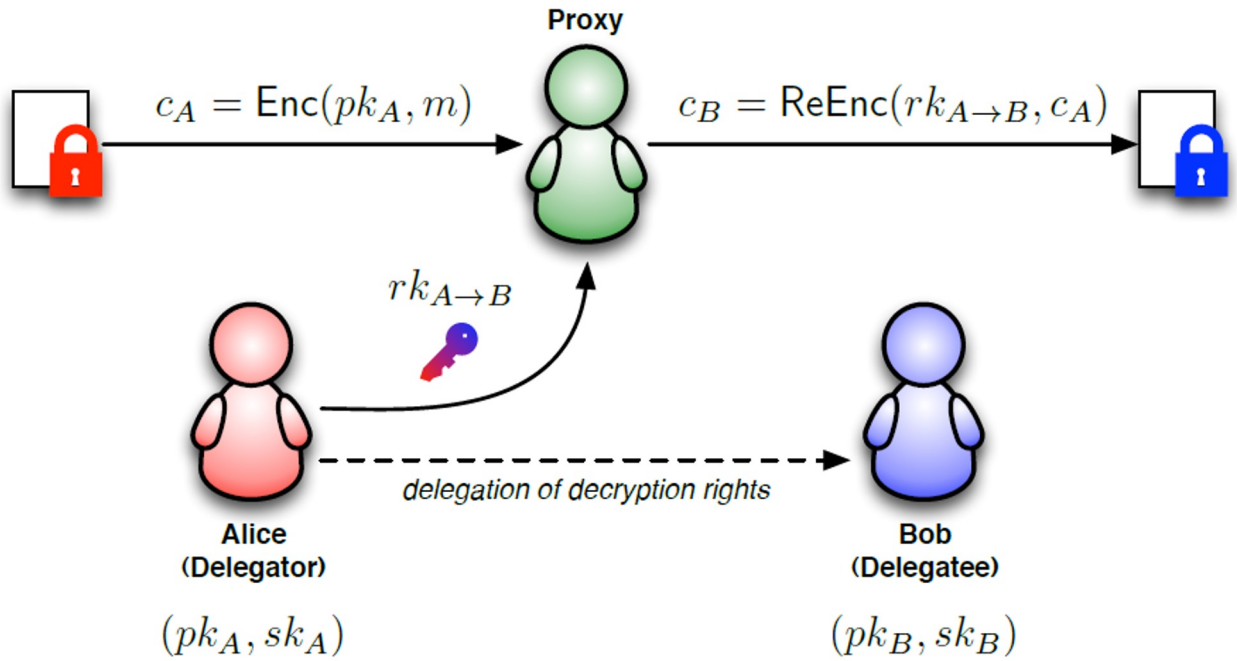
Tecnologías utilizadas



IPFS

- Direccionamiento por Contenido
- Identificador CID, hash del contenido
- Reduce el coste de almacenamiento.
- Hemos usado Infura IPFS gateway.
- Servicio de pinning 6 meses desde último acceso.

Proxy Reencryption



NuCypher

Proxy de reencriptación

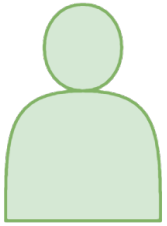
- Proxy de Reencriptación umbral (PRE).
- Utilizando criptografía asimétrica de curva elíptica.
- Transforma un ítem cifrado con la clave pública de Alice en un ítem cifrado que podría ser abierto únicamente usando la clave privada de Bob
- Sin necesidad de intercambiar ninguna clave privada entre los usuarios.
- Gestión soberana de los datos. Los propietarios consiguen el control total de su información.

Protocolo Propuesto

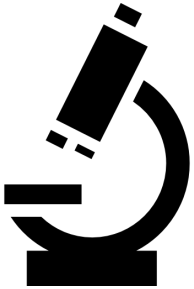
Actores

Regulatory authority

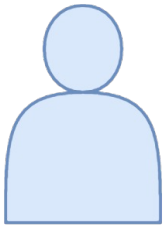
World Health Organization



User



Laboratory

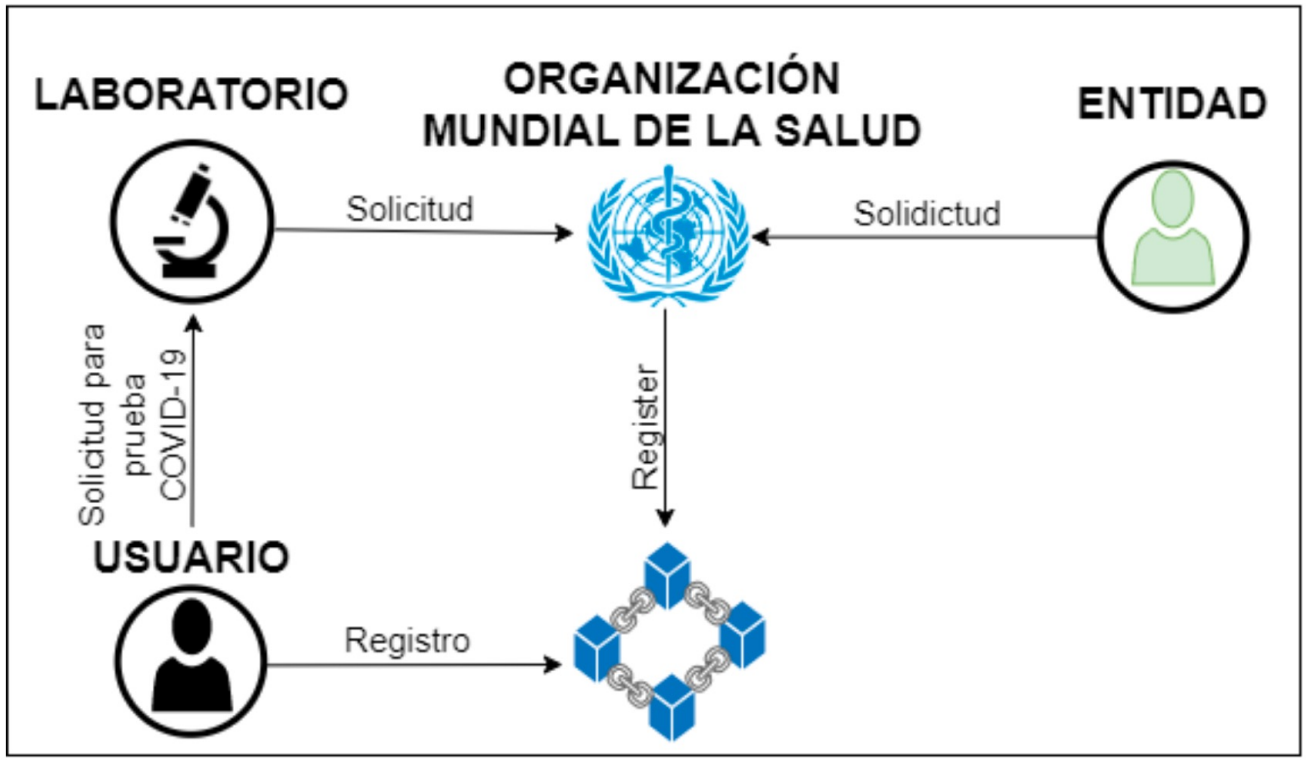


Trusted entity

Non – Trusted entity

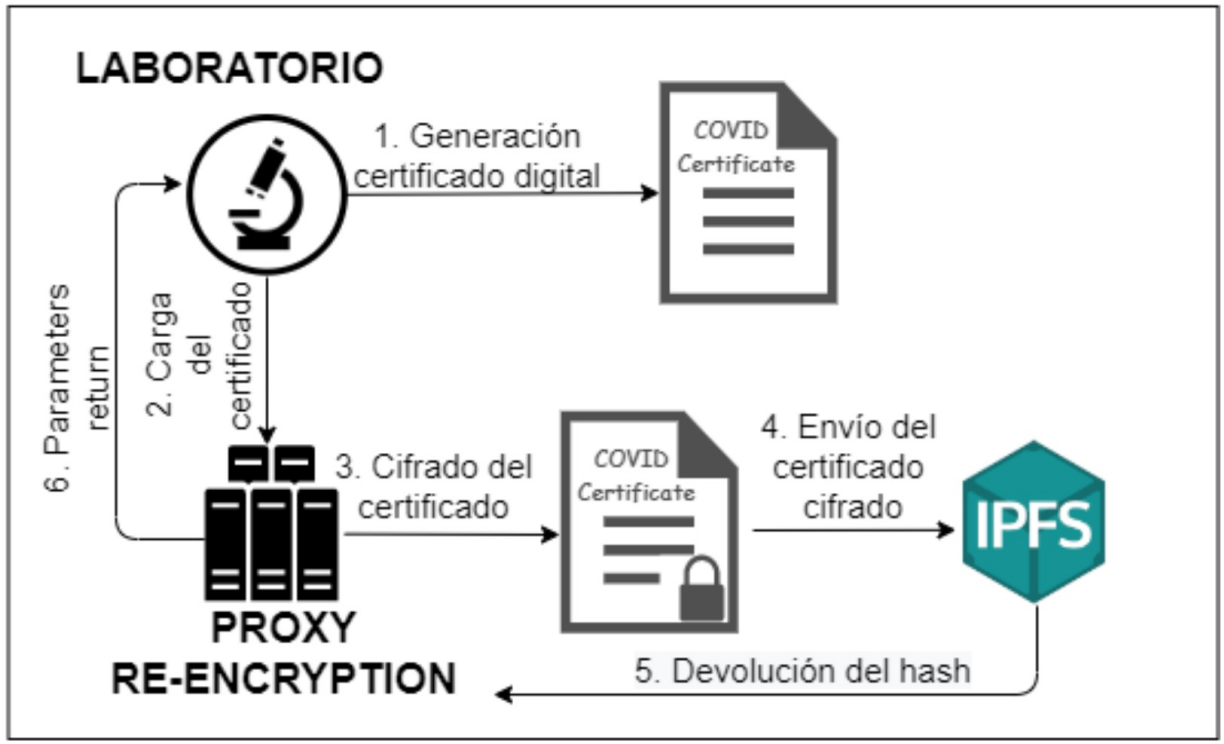
Protocolo

1. Registro de actores

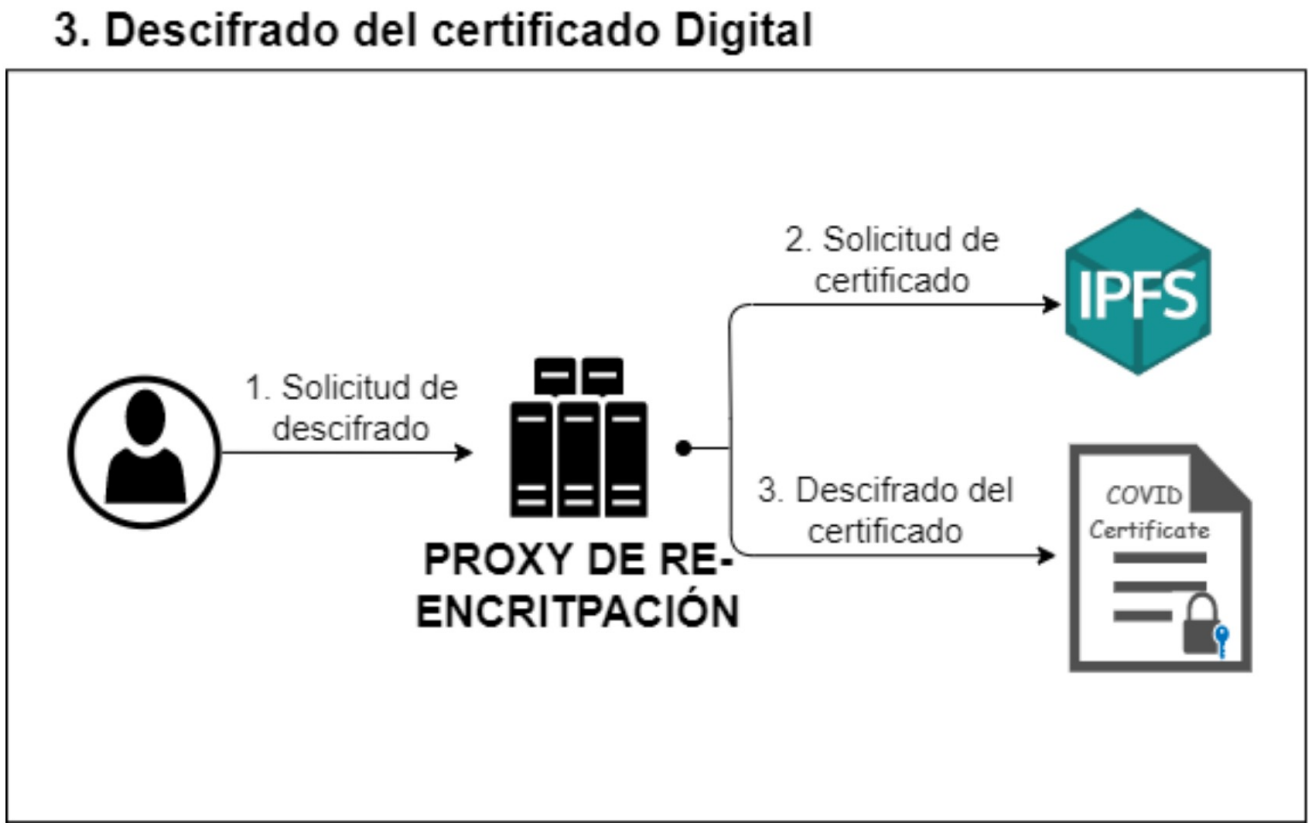


Protocolo

2. Generación certificado Digital

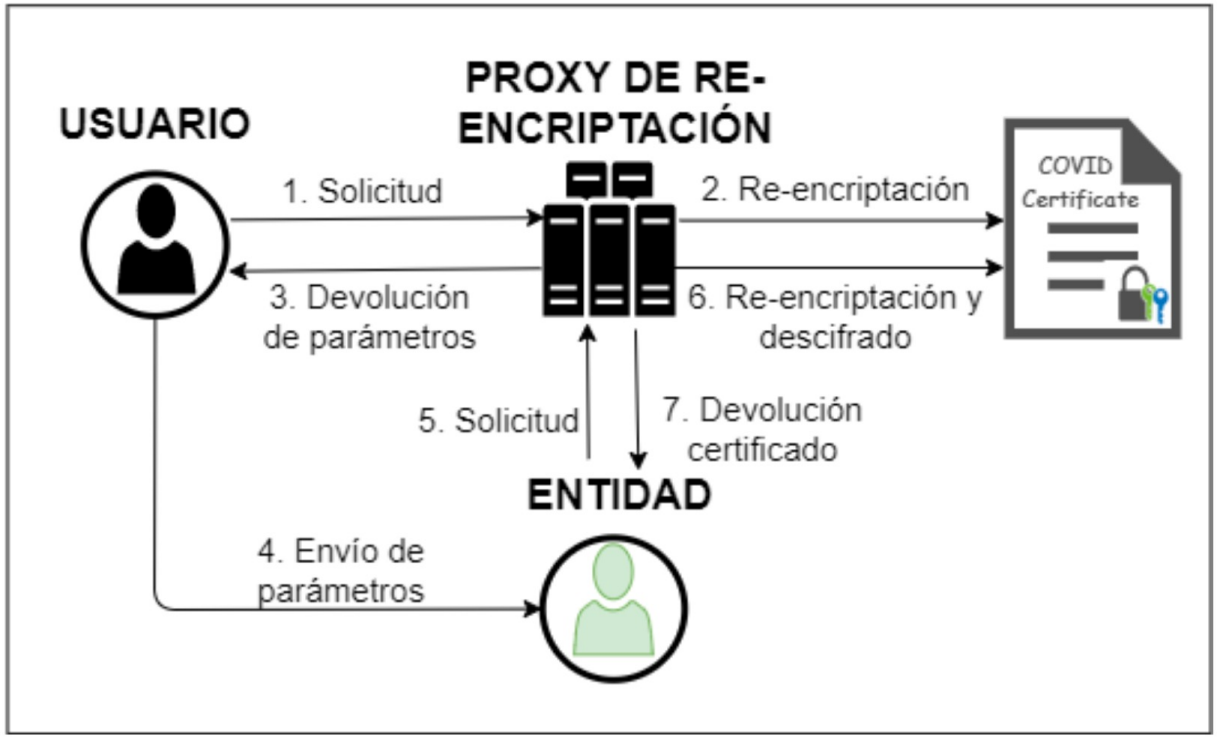


Protocolo


3. Descifrado del certificado Digital
1. Solicitud de descifrado
2. Solicitud de certificado
3. Descifrado del certificado
IPFS
COVID Certificate
PROXY DE RE-ENCRITPACIÓN

Protocolo

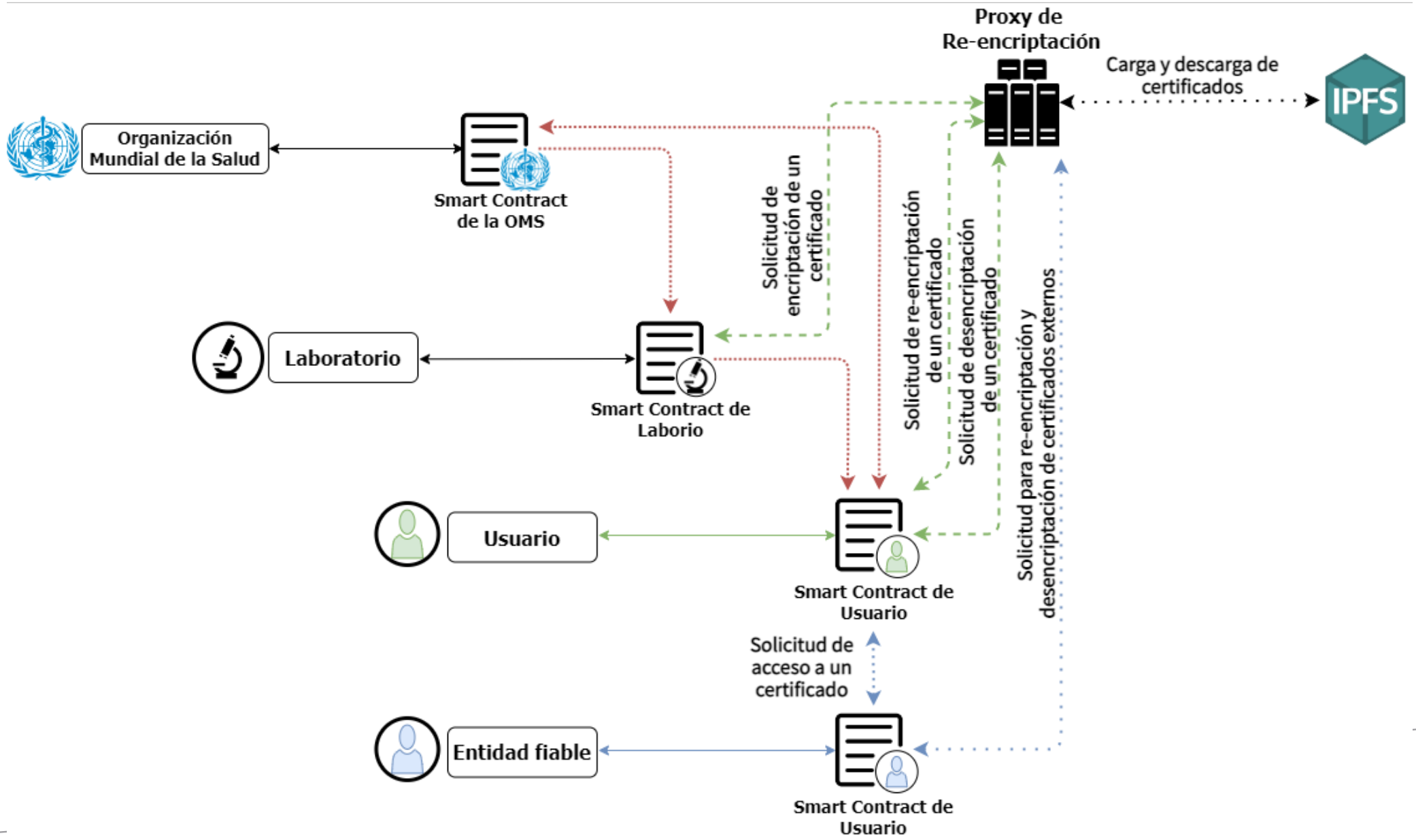
4. Compartición del certificado Digital



Smart Contracts

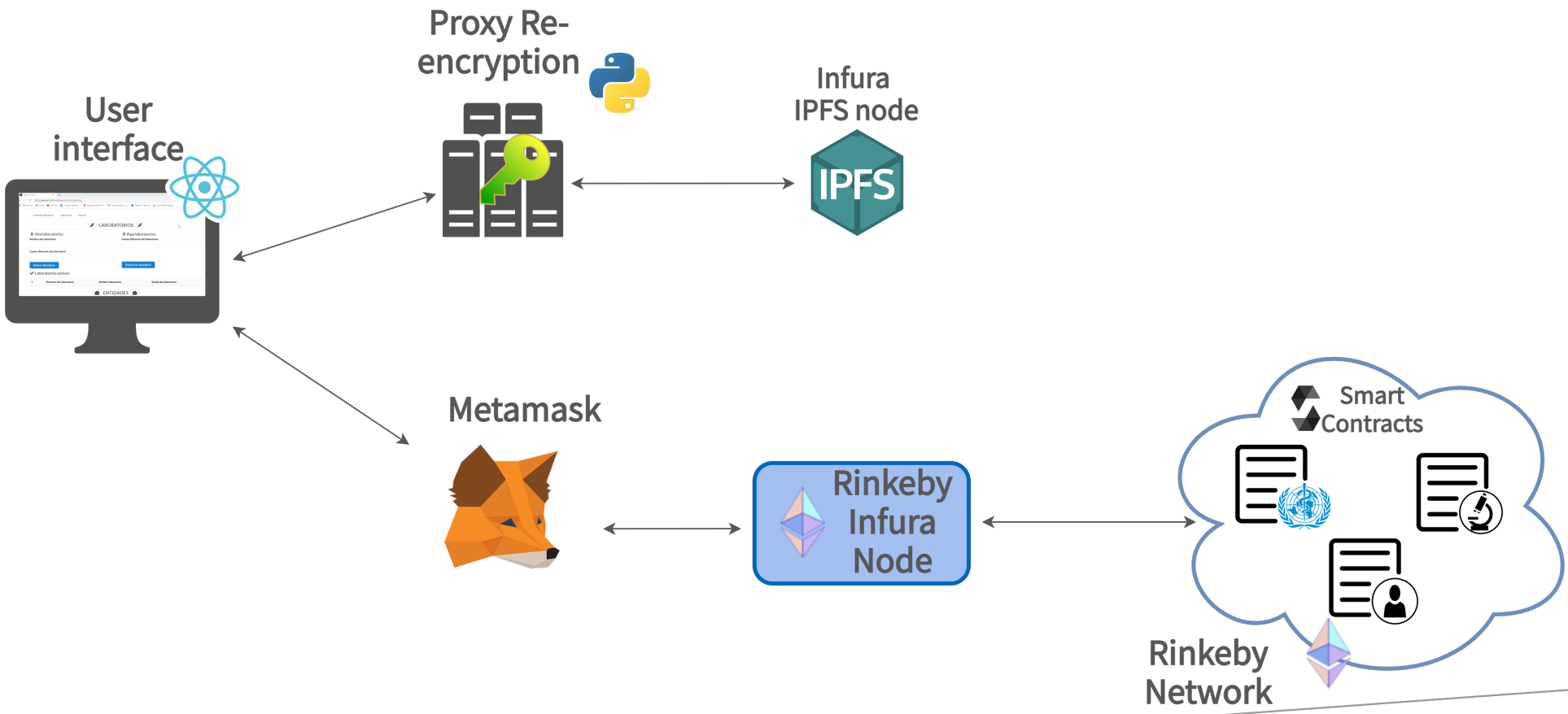
Funcionalidades

1. Gestión de laboratorios
2. Registro de usuarios
3. Gestión de entitadades fiables
4. Generación de certificados
5. Desencriptación por parte del propietario.
6. Compartición de certificados
7. Desencriptación de certificados externos.

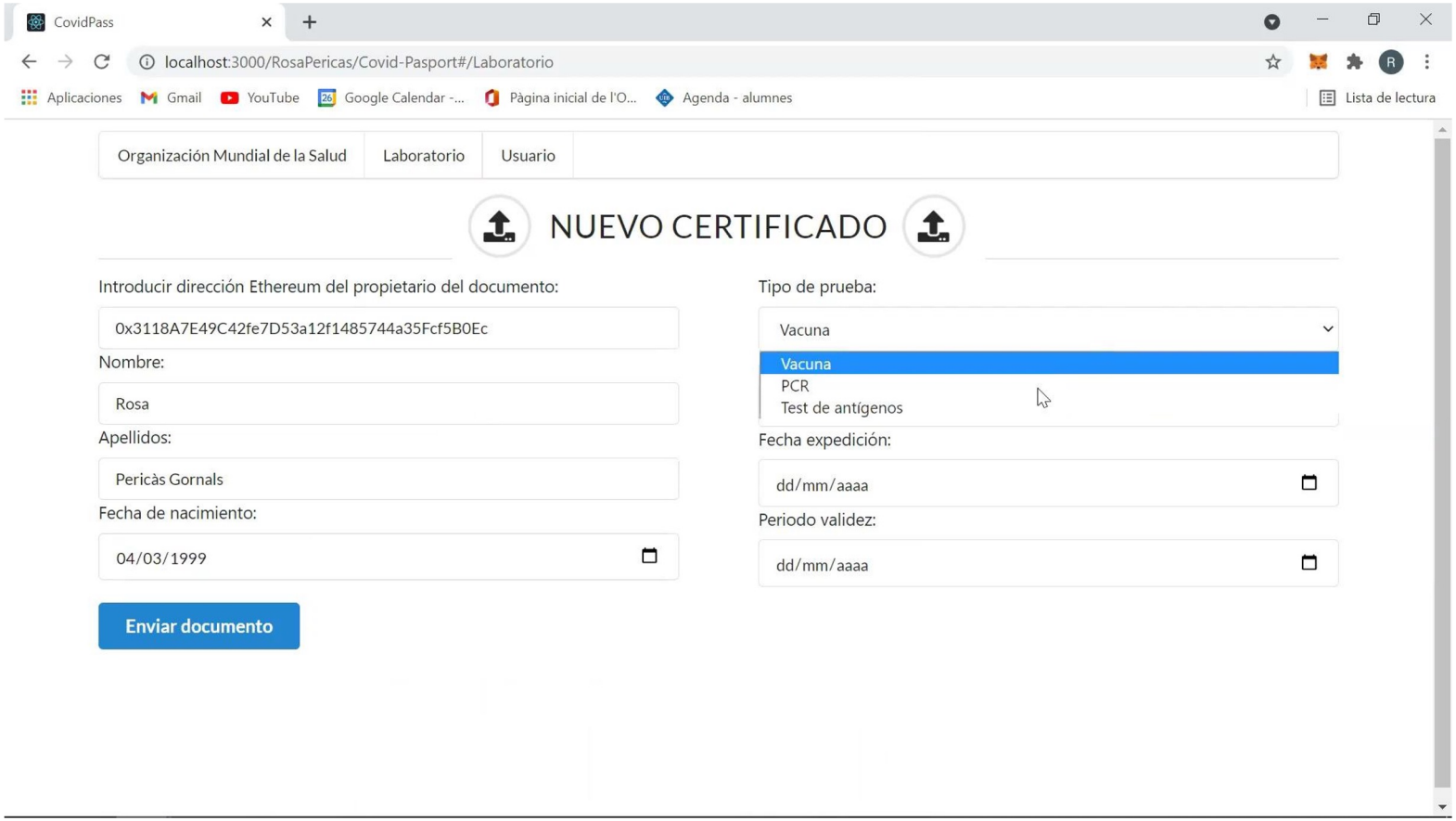

Proxy de
Re-encriptación
Carga y descarga de
certificados
IPFS
Organización
Mundial de la Salud
Smart Contract
de la OMS
Solicitud de
encriptación de un
certificado
Solicitud de re-encriptación
de un certificado
Solicitud de desencriptación
de un certificado
Solicitud para re-encriptación y
desencriptación de certificados externos
Laboratorio
Smart Contract de
Laborio
Usuario
Smart Contract de
Usuario
Solicitud de
acceso a un
certificado
Entidad fiable
Smart Contract de
Usuario

Implementación

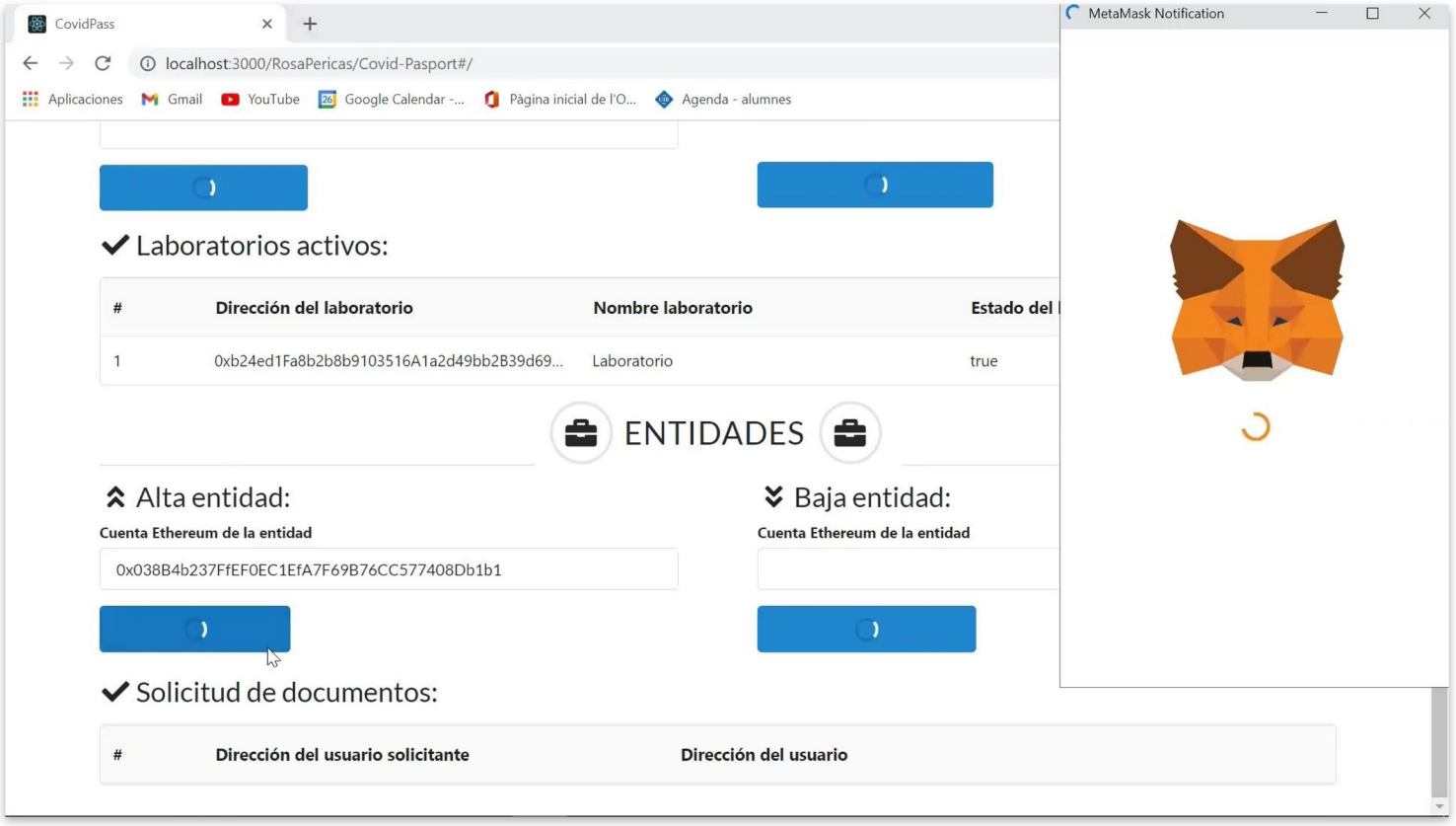
Implementación



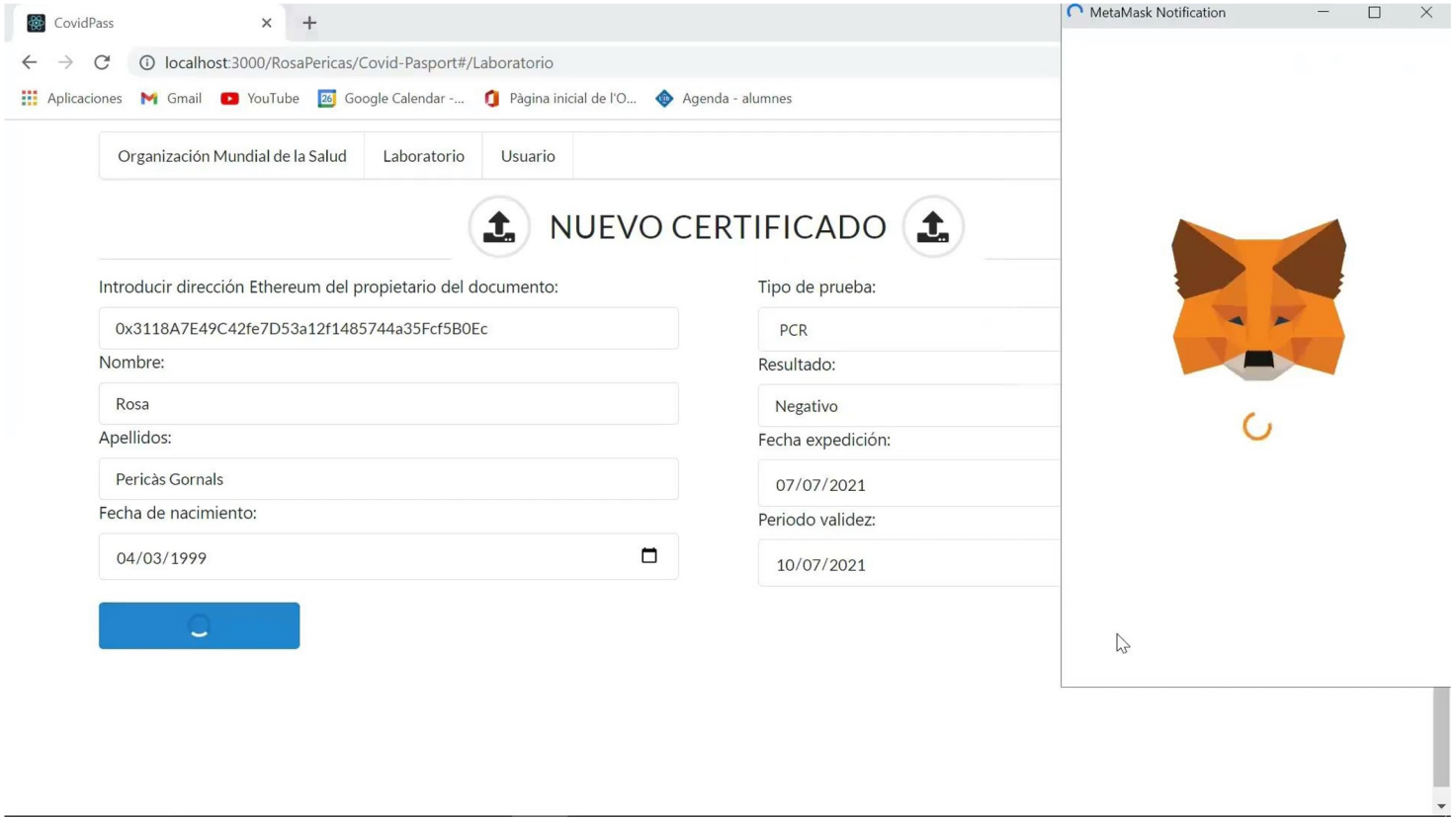
Front-End de generación de certificado



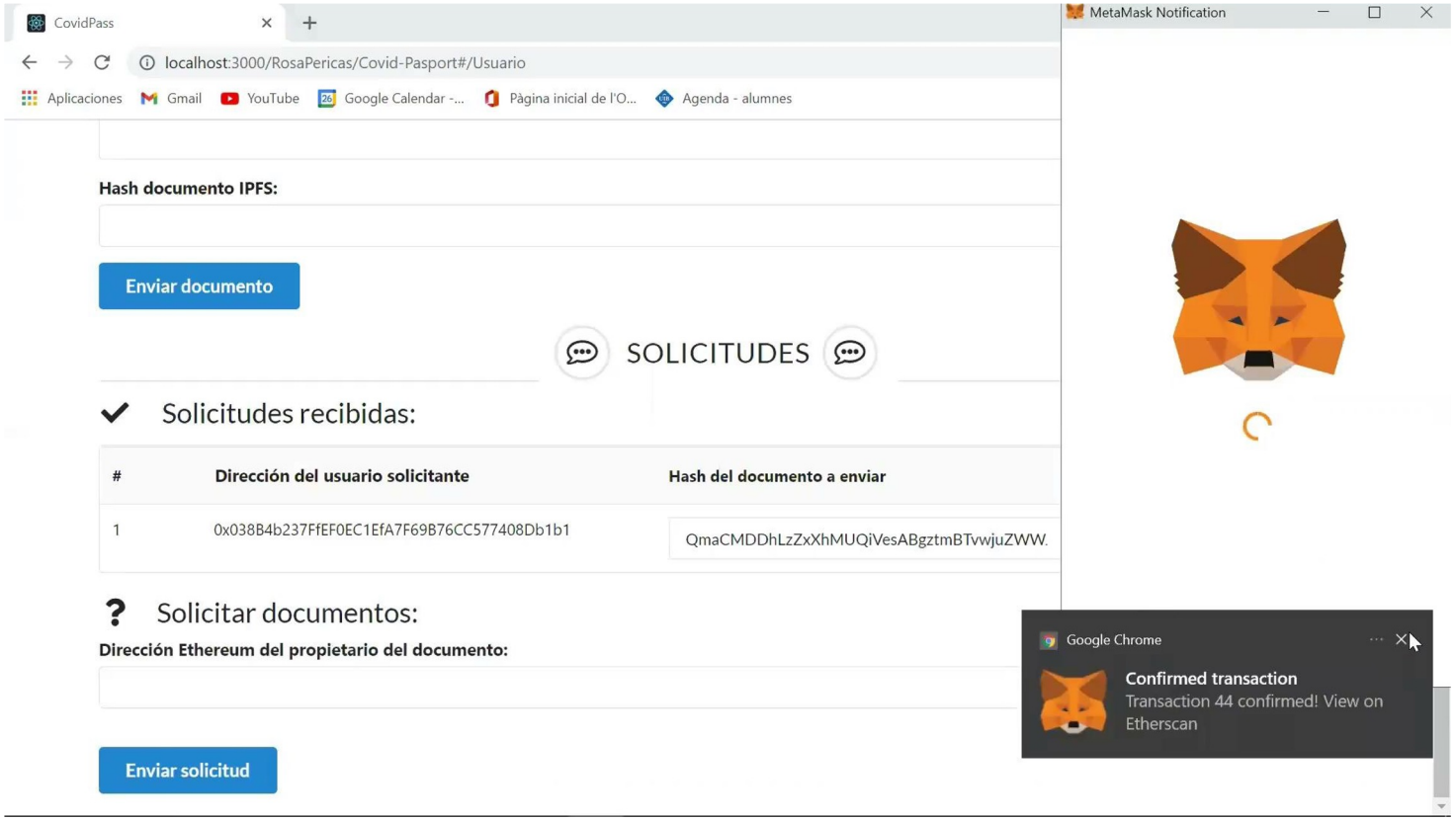
Alta y Baja de Entidades



Expedición del certificado



Acceso al certificado



Análisis de Seguridad

Propiedades

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticación
- No Repudio
- Soberanía
- Inmutabilidad
- Auditabilidad
- Autorization
- Trazabilidad

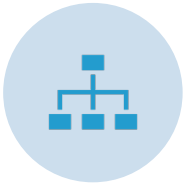
Análisis de Viabilidad

Análisis de Coste

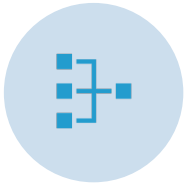
Function	Gas (wei)	USD (1 Gwei)	USD (10 Gwei)
Regulatory Autority	4913478	9,04	90,42
User Registration	2687489	4,95	49,45
Laboratory addition	416236	0,77	7,66
Laboratory removal	24834	0,05	0,47
Certificate generation	312792	0,58	5,76
Entity management	36099	0,07	0,66
Certificate sharing	868014	1,6	15,97

Costs results obtained on 27 June 2021, when 1 Eth = $1840,36

Conclusiones



Supervisión de emisores y validadores.



Descentralización.

Acceso permanente a los certficados.

Asegura la confidencialidad y la privacidad.

Adaptable a uso con diferentes datos sanitarios, como EHRs (Electronic Health Records).

https://github.com/secomuib/HighlyPrivateManagementSystemForDigitalCOVID-19Certificates

Universitat de les Illes Balears

Universitat de les Illes Balears

Sistema de gestión de certificados digitales COVID-19 basado en Blockchain

Rosa Pericàs Gornals

Macià Mut Puigserver

M. Magdalena Payeras Capellà

Llorenç Huguet Rotger