

Carlos Martinez · Mariana Brachetta · Julio Monetti · Alberto Cortez

LITAPS - Ingeniería en Sistemas de Información · UTN Facultad Regional Mendoza, Argentina

HL7 FHIR

SSI / DIDs / VCs

IPS

IHE Profiles

Ethereum L1

zkSync L2

ZK-Rollups

DSRM

## Resumen

La interoperabilidad en salud digital basada en HL7 FHIR está limitada por modelos de identidad centralizados que fragmentan la información del paciente. Esta investigación propone una arquitectura SSI que permite compartir el IPS y recursos FHIR mediante consentimiento granular y mecanismos criptográficos.

Integra estándares W3C (DIDs y Verifiable Credentials) con perfiles IHE, anclando confianza en Ethereum L1 y empleando zkSync L2 para operar con escalabilidad y eficiencia de costos.

## Problema e Introducción

### Brechas estructurales

- Modelos de identidad centralizados que fragmentan registros clínicos
- El paciente no controla la portabilidad de su información
- Verificación delegada a intermediarios, incrementando costos
- IPS e inmunizaciones: validación lenta entre jurisdicciones
- Duplicación de registros y errores de identificación

### SSI como solución

Los W3C DIDs permiten identificación descentralizada. Las Verifiable Credentials habilitan credenciales firmadas criptográficamente, verificables sin sincronía constante con el emisor.

## Líneas de Investigación y Desarrollo

### Marco metodológico: DSRM

Desde identificación del problema hasta la evaluación del prototipo.

### Ejes principales

- Arquitectura W3C DIDs + VCs para intercambio seguro de IPS y recursos FHIR
- Integración de perfiles IHE: PDQm, MHD y SVCM para interoperabilidad técnica y semántica
- Escalabilidad y eficiencia de costos en operaciones de identidad con zkSync L2
- Validación de portabilidad del IPS y certificados sanitarios en movilidad interjurisdiccional

## Formación de Recursos Humanos

El proyecto se desarrolla en LITAPS (UTN-FRM), integrando docentes investigadores, graduados, alumnos de grado y becarios.

### Impacto previsto

- Actualización curricular: Desarrollo de Software, Seguridad, Paradigmas de Programación
- Capacitación en modelado, desarrollo, integración y testing del prototipo
- Becarios con responsabilidades técnicas específicas
- Apoyo a TFG y proyección a tesis de posgrado
- Colaboración interdisciplinaria con expertos del dominio sanitario para la validación aplicada del prototipo.

## Arquitectura de Referencia Multicapa

 **Capa de Presentación** Wallet Digital – Holder (Paciente)

 **Capa Clínica** HL7 FHIR / IPS + IHE: PDQm · MHD · SVCM

 **Identity Connector** Puente SSI ↔ Sistemas Legados de Salud

 **Capa SSI** W3C DIDs · Verifiable Credentials · ZK-Proofs

 **Capa L2 – zkSync (ZK-Rollup)** Emisión · Verificación · Revocación

 **Capa L1 – Ethereum** Smart Contracts · Ancla de Confianza · PHI off-chain

★ PHI se mantiene OFF-CHAIN – solo hashes e identificadores residen en blockchain

W3C DID Core

W3C VC 1.1

HL7 FHIR R4

IHE PDQm

IHE MHD

IHE SVCM

## Resultados Obtenidos

### A · Arquitectura Multicapa

Privacidad por diseño (PHI off-chain). Wallet del paciente (Holder), servicios FHIR/IPS (Issuer), Identity Connector y anclaje en Ethereum L1 con escalabilidad en zkSync L2.

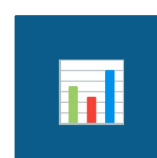
### B · Laboratorio de Pruebas

IPS National Backend (RACSEL-LACPASS) contenerizado. Núcleos FHIR, terminología SNOMED CT, mediación IHE MHD y servicios VHL (Verifiable Health Links).

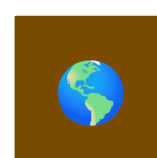
## Resultados Esperados



**Validación técnica:** Integridad criptográfica y verificación de estado de credenciales sobre infraestructura L1/L2.



**Métricas de desempeño:** Latencia, tasas de éxito y viabilidad económica mediante optimización de costos en zkSync.



**Escenarios de movilidad:** Portabilidad del IPS para continuidad asistencial y verificación de certificados sanitarios.