Patient-Centered Interoperability: An Architecture for Sharing the Health Summary Using Decentralized Digital Identity and Verifiable Credentials with Blockchain

Carlos Martínez[1,2][0000-0001-7100-7515], Mariana Brachetta[1,2][0000-0003-3388-0326], Julio Monetti[1,2][0000-0002-2148-146X], and Alberto Cortez[1,2][0000-0001-9003-050X]

[1]Laboratorio de Integración de Tecnologías Aplicadas a Prototipos de Software (LITAPS),
[2]Ingeniería en Sistemas de Información, UTN Facultad Regional Mendoza, Argentina
{carlos.martinez, mariana.brachetta, julio.monetti, alberto.cortez}@docentes.frm.utn.edu.ar

Abstract. Digital health interoperability, supported by standards such as HL7 FHIR, remains constrained by centralized identity models that fragment clinical information and hinder data portability across healthcare providers. This fragmentation is particularly acute in cross-jurisdictional scenarios involving the International Patient Summary (IPS), where reliance on institutional intermediaries increases costs, duplication, and inconsistency risks. This work proposes and validates a architecture that integrates Self-Sovereign Identity (SSI) with clinical interoperability standards to enable patient-centered health data exchange. The architecture is organized into six layers: a presentation layer with a patient digital wallet (Holder); a clinical interoperability layer based on HL7 FHIR R4, IPS, and IHE profiles (PDQm, MHD, SVCM); an Identity Connector middleware bridging legacy EHR/FHIR systems with the SSI ecosystem; an SSI layer implementing W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) with zero-knowledge proofs; a Layer 2 execution layer on zkSync (ZK-rollup) for identity operations; and a Layer 1 trust anchor on Ethereum via smart contracts, ensuring that Protected Health Information (PHI) remains off-chain. A functional test laboratory was deployed based on the RACSEL–IPS National Backend containerized stack, enabling validation of IPS–FHIR flows and IHE profile integration. Preliminary results confirm the technical feasibility of the proposed architecture and show that delegating identity operations to a ZK-rollup reduces on-chain data exposure and is expected to yield substantial gas savings compared with Ethereum Mainnet for sovereign, scalable, and privacy-preserving clinical data exchange.

Keywords. Health Interoperability, Self-Sovereign Identity (SSI), HL7 FHIR, International Patient Summary (IPS), Verifiable Credentials (VCs).

Interoperabilidad Centrada en el Paciente: Arquitectura para Compartir el Resumen de Salud mediante Identidad Digital Descentralizada y Credenciales Verificables con Blockchain

Resumen. La interoperabilidad en salud digital, sustentada en estándares como HL7 FHIR, continúa limitada por modelos de identidad centralizados que fragmentan la información clínica y dificultan la portabilidad de datos entre efectores de salud. Esta fragmentación resulta particularmente crítica en escenarios interjurisdiccionales que involucran el Resumen Internacional del Paciente (IPS), donde la dependencia de intermediarios institucionales incrementa costos, duplicaciones e inconsistencias. Este trabajo propone y valida una arquitectura que integra Identidad Auto-Soberana (SSI) con estándares de interoperabilidad clínica para habilitar un intercambio de datos de salud centrado en el paciente. La arquitectura se organiza en seis capas: una capa de presentación con wallet digital del paciente (Holder); una capa de interoperabilidad clínica basada en HL7 FHIR R4, IPS y perfiles IHE (PDQm, MHD, SVCM); un middleware Identity Connector que conecta sistemas legados EHR/FHIR con el ecosistema SSI; una capa SSI que implementa W3C Decentralized Identifiers (DIDs) y Verifiable Credentials (VCs) con pruebas de conocimiento cero; una capa de ejecución en Capa 2 sobre zkSync (ZK-rollup) para operaciones de identidad; y un ancla de confianza en Capa 1 sobre Ethereum mediante contratos inteligentes, asegurando que la Información Clínica Protegida (PHI) permanezca fuera de la cadena. Se desplegó un laboratorio de pruebas funcional basado en el stack contenerizado RACSEL–IPS National Backend, habilitando la validación de flujos IPS–FHIR e integración con perfiles IHE. Los resultados preliminares confirman la viabilidad técnica de la arquitectura propuesta y muestran que delegar las operaciones de identidad en un ZK-rollup reduce la exposición de datos on-chain, con un ahorro de gas estimado considerable respecto de Ethereum Mainnet, para un intercambio clínico soberano, escalable y con preservación de la privacidad.

Palabras clave. Interoperabilidad en Salud, Identidad Auto-Soberana (SSI), HL7 FHIR, Resumen Internacional del Paciente (IPS), Verifiable Credentials (VCs).

1 Introducción

En los últimos años, la interoperabilidad en salud digital ha cobrado relevancia estratégica por el aumento de la movilidad de los pacientes, la continuidad del cuidado y la necesidad de intercambio oportuno de información clínica entre instituciones. La adopción de estándares como HL7 FHIR ha impulsado interfaces modernas para representar, consultar e intercambiar recursos clínicos de forma

estructurada, y ha fortalecido perfiles orientados al intercambio transfronterizo, como el International Patient Summary (IPS), concebido como un conjunto mínimo de datos clínicos esenciales para escenarios interjurisdiccionales (HL7, s. f.a; HL7, s. f.b).

Sin embargo, persisten brechas estructurales asociadas a modelos de gestión y validación de identidad centralizados y a esquemas de intercambio donde el paciente no controla de forma directa la portabilidad de su información. En la práctica, esto contribuye a la fragmentación de registros, dificulta la conciliación clínica entre efectores y traslada la verificación a intermediarios institucionales, muchas veces con limitaciones respecto del marco regulatorio vigente. El problema se evidencia especialmente en contextos regionales e internacionales, donde la validación de inmunizaciones y el intercambio del IPS pueden volverse lentos o inconsistentes, incrementando costos operativos, duplicación de registros y riesgos de errores de identificación o de reconciliación de datos.

Para abordar estas limitaciones, investigaciones recientes proponen la Identidad Auto-Soberana (Self-Sovereign Identity, SSI) como un enfoque centrado en la persona, en el cual el control de las credenciales se desplaza a una wallet digital y la confianza se sustenta en estándares abiertos. En este paradigma, los W3C Decentralized Identifiers (DIDs) posibilitan la identificación descentralizada de personas e instituciones, mientras que las W3C Verifiable Credentials (VCs) habilitan credenciales firmadas criptográficamente, verificables y a prueba de manipulaciones, reduciendo la dependencia de verificaciones sincrónicas con el emisor en cada transacción (W3C, 2022a; W3C, 2022b). En el ámbito sanitario, se han reportado marcos SSI aplicados a credenciales y a la gestión de tarjetas de salud electrónicas, con mejoras en privacidad e interoperabilidad frente a modelos convencionales (Salah et al., 2025). Asimismo, otros trabajos exploran plataformas y modelos SSI para salud centrada en el paciente, apoyados en blockchain y orientados al cumplimiento de regulaciones de protección de datos (de Siqueira et al., 2021; Bai et al., 2022; Harrell et al., 2022).

A diferencia de estos aportes —que suelen concentrarse en el modelo SSI y su aplicación a credenciales sanitarias—, la presente propuesta se enfoca en la definición y validación de una arquitectura para el intercambio interjurisdiccional de información clínica conforme a HL7 FHIR, particularmente el IPS, integrando SSI con perfiles IHE que operacionalizan la interoperabilidad técnica y semántica: PDQm, MHD y SVCM (IHE, s. f.a; IHE, s. f.b; IHE, s. f.c). En este marco, el uso de blockchain resulta necesario por tres razones: (i) proveer un ancla de confianza inmutable y auditable para el registro raíz de emisores autorizados y las políticas de revocación; (ii) habilitar verificaciones sin necesidad de confiar en un único intermediario institucional; y (iii) garantizar disponibilidad y trazabilidad de los eventos de emisión y revocación de credenciales. No obstante, el costo transaccional de Ethereum Mainnet dificulta su aplicación a escala sanitaria, donde el volumen de emisiones, verificaciones y revocaciones puede ser elevado. Este problema de escalabilidad justifica el uso de una solución de Capa 2 (L2). Concretamente, se propone anclar la confianza en Ethereum (Capa 1) (Ethereum, s. f.) y emplear zkSync (Capa 2, ZK-rollup) (Matter Labs, s. f.) para soportar operaciones de identidad de alta

frecuencia —incluyendo emisión, verificación y revocación— con costos marginales y garantías criptográficas heredadas de la cadena principal.

La contribución central de este trabajo consiste en proponer y validar una arquitectura de seis capas que integra SSI (DIDs/VCs) con HL7 FHIR e IHE (PDQm, MHD, SVCM), habilitando un intercambio clínico centrado en el paciente. Dicha arquitectura permite al paciente compartir, bajo consentimiento granular, su IPS o recursos FHIR específicos de forma segura y selectiva entre efectores de salud de distintas jurisdicciones, preservando la privacidad y soberanía de los datos con escalabilidad y eficiencia de costos. Adicionalmente, se incorporan mecanismos de criptografía avanzada —pruebas de conocimiento cero (Zero-Knowledge Proofs, ZKP)— que permiten la validación de afirmaciones sin exposición de la información clínica subyacente.

El resto del artículo se organiza de la siguiente manera. La Sección 2 presenta los trabajos relacionados y el posicionamiento frente al estado del arte. La Sección 3 detalla la metodología adoptada y la arquitectura propuesta de seis capas. La Sección 4 describe los resultados obtenidos, incluyendo el laboratorio de pruebas desplegado. La Sección 5 discute los hallazgos, las limitaciones y los resultados esperados. Finalmente, la Sección 6 presenta las conclusiones y las líneas de trabajo futuro.

2 Trabajos Relacionados

La interoperabilidad en salud digital y la gestión descentralizada de identidades clínicas han sido objeto de creciente interés académico. Este apartado analiza críticamente la literatura relevante, organizándola en tres ejes temáticos: SSI aplicada al dominio sanitario, interoperabilidad clínica basada en HL7 FHIR/IPS, y blockchain como infraestructura de confianza.

SSI en el dominio sanitario. Diversos estudios han explorado la aplicación de SSI al sector salud. de Siqueira et al. (2021) presentan un enfoque de datos de salud centrado en el usuario mediante identidades auto-soberanas. Bai et al. (2022) proponen un modelo de gestión de identidad auto-soberana para sistemas de salud inteligentes, basado en sensores y blockchain, con énfasis en la privacidad del paciente, mientras que Harrell et al. (2022) describen el diseño técnico de una plataforma SSI para atención médica centrada en el paciente utilizando tecnología blockchain. Más recientemente, Salah et al. (2025) abordan la gestión de tarjetas de salud electrónicas mediante identidad digital auto-soberana en sistemas basados en blockchain. Sin embargo, estos trabajos se concentran predominantemente en el modelo de identidad y credenciales, sin integrar de forma explícita estándares de interoperabilidad clínica como HL7 FHIR o perfiles IHE para el intercambio efectivo de información sanitaria estructurada. Tampoco abordan la materialización de estas arquitecturas en entornos de laboratorio reproducibles que permitan la validación experimental de los flujos propuestos.

Interoperabilidad clínica con HL7 FHIR e IPS. El estándar HL7 FHIR (HL7, s. f.b) se ha consolidado como la base para el intercambio moderno de datos clínicos, y el International Patient Summary (HL7, s. f.a) define un conjunto mínimo de datos esenciales para la continuidad asistencial transfronteriza. Los perfiles IHE —PDQm para consultas demográficas móviles (IHE, s. f.a), MHD para acceso móvil a

documentos clínicos (IHE, s. f.b) y SVCM para armonización terminológica (IHE, s. f.c)— complementan FHIR en escenarios de interoperabilidad real. No obstante, la literatura existente rara vez combina estos perfiles con modelos SSI, dejando un vacío en la operacionalización de la identidad descentralizada dentro de flujos clínicos estandarizados.

Blockchain como infraestructura de confianza. El uso de blockchain para anclar marcos de confianza en salud ha sido abordado desde diversas perspectivas. Ethereum (Ethereum, s. f.) provee una capa de confianza inmutable, pero su costo transaccional limita la adopción a escala. Soluciones de Capa 2 como zkSync (Matter Labs, s. f.) ofrecen mayor eficiencia mediante ZK-rollups, manteniendo las garantías de seguridad de la cadena principal. Adicionalmente, la integración de pruebas de conocimiento cero (ZKP) permite verificar matemáticamente la validez, integridad y autoría de un consentimiento sin revelar los metadatos de la transacción ni el contenido clínico subyacente (Sasson et al., 2014). A pesar de estos avances, la integración explícita de L1/L2 con estándares SSI y flujos clínicos FHIR/IPS no ha sido abordada de forma sistemática en la literatura revisada, y menos aún en entornos de laboratorio que permitan su validación experimental.

La Tabla 1 sintetiza el análisis comparativo del estado del arte respecto de las dimensiones relevantes para esta investigación y posiciona la propuesta presentada.

Tabla 1. Análisis comparativo del estado del arte y posicionamiento de la propuesta.

Referencia	Enfoque SSI (DIDs/VCs)	HL7 FHIR / IPS	Perfiles IHE	L2 / ZKP	Laboratorio reproducible
Bai et al. (2022)	Sí	No	No	No	Parcial
de Siqueira et al. (2021)	Sí	No	No	No	No
Harrell et al. (2022)	Sí	Parcial	No	No	No
Salah et al. (2025)	Sí	No	No	No	No
RACSEL–LACP ASS (s. f.)	No	Sí	Sí	No	Sí
Nuestra propuesta	Sí	Sí	Sí	Sí	Sí

En síntesis, si bien existen aportes significativos en cada eje individual, se identifica un vacío en la integración articulada de SSI (DIDs/VCs), estándares de interoperabilidad clínica (HL7 FHIR, IPS, perfiles IHE) y una infraestructura blockchain L1/L2 eficiente, materializada en una arquitectura reproducible para el intercambio interjurisdiccional de información sanitaria centrado en el paciente. La presente investigación se posiciona precisamente en esa intersección.

3 Metodología

La investigación adopta la Investigación en Ciencia del Diseño (Design Science Research Methodology, DSRM) (Haryanti et al., 2022) como marco metodológico,

debido a su cobertura integral del ciclo de construcción de artefactos —desde la definición del problema hasta la evaluación—, lo que resulta particularmente idóneo para investigaciones en Sistemas de Información orientadas a prototipos. El objetivo central es diseñar, implementar y evaluar una arquitectura que demuestre la viabilidad de un sistema basado en los estándares W3C DIDs y VCs (W3C, 2022a; W3C, 2022b), aplicado al intercambio seguro de información clínica conforme a HL7 FHIR R4 (HL7, s. f.b) y al IPS (HL7, s. f.a), integrando los perfiles IHE (PDQm, MHD y SVCM) para garantizar la interoperabilidad técnica y semántica (IHE, s. f.a; IHE, s. f.b; IHE, s. f.c). El presente artículo cubre de forma exhaustiva las fases de Identificación del problema, Definición de objetivos y Diseño/Desarrollo del artefacto, y presenta resultados preliminares de la fase de Demostración.

3.1 Etapas DSRM

La investigación se estructura en las siguientes etapas conforme a DSRM. En la etapa de identificación del problema se analiza la fragmentación de datos clínicos, las dificultades de verificación interjurisdiccional y la dependencia de intermediarios institucionales en el intercambio de información sanitaria. La definición de objetivos establece los requisitos de consentimiento granular, privacidad por diseño (PHI off-chain), trazabilidad técnica, escalabilidad y eficiencia de costos operativos. En la etapa de diseño y desarrollo se define la arquitectura de seis capas y se construye el prototipo integrado sobre infraestructura contenerizada. La etapa de demostración contempla la ejecución de casos de uso del ciclo Issuer–Holder–Verifier en escenarios de movilidad y verificación de certificados sanitarios. Finalmente, la evaluación incluye la validación de propiedades criptográficas, verificación de no-revocación, métricas de latencia y costo, y cumplimiento de privacidad (Bai et al., 2022; Harrell et al., 2022).

3.2 Arquitectura propuesta

La arquitectura propuesta se organiza en seis capas lógicas que articulan la soberanía del paciente, la interoperabilidad clínica, la gestión de identidad descentralizada y la confianza basada en blockchain (Fig. 1). A diferencia de propuestas previas que operan con tres capas genéricas (Issuer–Holder–Verifier), esta arquitectura descompone explícitamente las responsabilidades en capas especializadas, facilitando la modularidad, la reproducibilidad del entorno de pruebas y la validación independiente de cada componente. A continuación se describe cada capa, desde la interfaz del paciente hasta la infraestructura de confianza.

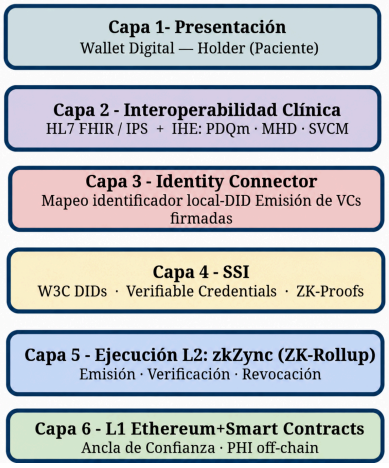

Fig. 1. Arquitectura de seis capas para el intercambio del IPS basada en SSI, con ejecución en zkSync (Capa 2) y ancla de confianza en Ethereum (Capa 1). Toda la información clínica protegida se mantiene off-chain.

Capa 1 – Presentación: Wallet Digital (Holder). Esta capa constituye la interfaz del paciente con el ecosistema. Incorpora una wallet digital compatible con DIDs/VCs que permite la gestión de claves criptográficas, la autorización explícita del intercambio y la generación de Presentaciones Verificables (VP) minimizadas, compartiendo estrictamente los datos necesarios bajo consentimiento granular (W3C, 2022a; W3C, 2022b). El paciente define reglas específicas: qué efector accede, a qué segmento del IPS-FHIR (por ejemplo, alergias y medicación), y por cuánto tiempo. Esta capa materializa el principio de soberanía del dato, invirtiendo la pirámide de control: la información no pertenece a la institución que la genera, sino al paciente titular del DID.

Capa 2 – Interoperabilidad Clínica: HL7 FHIR/IPS + IHE. El núcleo clínico implementa servicios HL7 FHIR R4 sobre repositorios seguros off-chain (HL7, s. f.b). Integra perfiles IHE para interoperabilidad técnica y semántica: PDQm para consultas demográficas móviles y resolución de identidad (IHE, s. f.a); MHD (transacciones ITI-65/66/67/68) para publicación, búsqueda y recuperación de documentos clínicos (IHE, s. f.b); y SVCM para validación y compartición de artefactos terminológicos (IHE, s. f.c). La capa soporta la estructura del IPS (HL7, s. f.a) y asegura que el payload de datos clínicos se adhiera estrictamente al estándar FHIR, utilizando el perfil IPS para garantizar la interpretación inequívoca por sistemas heterogéneos globales. Los datos clínicos no persisten en la blockchain.

Capa 3 – Identity Connector: puente SSI ↔ sistemas legados. Se introduce un middleware que orquesta la integración entre los sistemas legados de salud (EHR/FHIR) y el ecosistema SSI. El Identity Connector cumple tres funciones técnicas principales. Primero, la autenticación frente al servidor FHIR se realiza mediante el perfil SMART on FHIR con flujos OAuth 2.0 (Authorization Code con PKCE) y scopes FHIR-específicos (por ejemplo, patient/Immunization.read o patient/AllergyIntolerance.read), lo que permite delegar al paciente la decisión de qué

porciones de su registro se exponen al Connector. Segundo, el Connector mantiene un mapeo interno entre el identificador local del paciente en el sistema clínico (típicamente un Patient.identifier resuelto vía PDQm) y el DID del paciente; este mapeo se materializa como una credencial interna emitida por la institución que no se publica on-chain. Tercero, una vez autorizado el acceso, el Connector extrae los recursos FHIR pertinentes, los empaqueta en una Credencial Verificable firmada con el DID institucional y publica únicamente el hash de la credencial en la Capa 5, dejando el payload clínico en el repositorio FHIR (Harrell et al., 2022).

Capa 4 – SSI: W3C DIDs, Verifiable Credentials y ZK-Proofs. Esta capa implementa el modelo de identidad descentralizada conforme a los estándares W3C. Los DIDs posibilitan la identificación descentralizada de pacientes e instituciones, y las VCs habilitan credenciales firmadas criptográficamente que encapsulan permisos granulares sobre el conjunto de datos clínicos (W3C, 2022a; W3C, 2022b). La validación de credenciales emplea ZK-SNARKs (Sasson et al., 2014): en lugar de presentar la credencial completa, la wallet genera una prueba que demuestra simultáneamente (i) que la credencial fue firmada por un emisor autorizado, (ii) que no ha sido revocada al momento de la verificación y (iii) que un atributo específico satisface una condición (por ejemplo, que la inmunización corresponde a un código SNOMED CT dentro del conjunto esperado), sin revelar los atributos restantes ni el identificador persistente del paciente. La revocación se gestiona mediante acumuladores criptográficos (RSA o basados en emparejamientos), cuyo estado se actualiza en Capa 5: este enfoque es preferible al almacenamiento de hashes estáticos porque permite probar no-pertenencia sin publicar un listado persistente de credenciales revocadas, alineándose mejor con el principio de minimización de datos y con el derecho al olvido exigido por GDPR.

Capa 5 – Ejecución L2: zkSync (ZK-Rollup). Las operaciones de identidad de alta frecuencia se ejecutan sobre zkSync (Matter Labs, s. f.), logrando costos transaccionales significativamente menores que en la cadena principal y mayor throughput. En esta arquitectura, zkSync desempeña un rol acotado y bien definido dentro del ecosistema SSI: (i) anclar el DID Document de emisores e instituciones mediante un método DID compatible con la L2 (por ejemplo did:ethr o did:pkh sobre zkSync), (ii) registrar el hash criptográfico (SHA-256) de cada credencial emitida para dotarla de integridad verificable, y (iii) administrar el estado del acumulador criptográfico de revocaciones. Las Credenciales Verificables propiamente dichas —documentos JSON-LD firmados— residen en la wallet del paciente y no se publican on-chain. Todo payload clínico permanece fuera de la cadena.

Capa 6 – Ancla de Confianza L1: Ethereum y Smart Contracts. Ethereum (Ethereum, s. f.) provee el ancla de confianza inmutable para el marco general. Los contratos inteligentes desplegados en L1 gestionan registros críticos: emisores autorizados, políticas de revocación y el registro raíz de confianza. La información clínica protegida (PHI) se mantiene estrictamente off-chain —solo hashes, identificadores de DID y commitments del acumulador residen en blockchain—, cumpliendo con los principios de minimización de datos propios de SSI y mitigando tensiones con regulaciones como GDPR e HIPAA mediante el uso de acumuladores (de Siqueira et al., 2021; Bai et al., 2022; Harrell et al., 2022).

3.3 Especificación del contrato inteligente de registro de credenciales

Para concretar el rol de la Capa 6, se especifica un contrato inteligente de registro de credenciales escrito en Solidity (Listado 1). El contrato mantiene dos estructuras: un registro de emisores autorizados por parte de la autoridad de gobernanza, y un mapeo de hashes de credenciales emitidas a su estado. Ambas operaciones (registro y revocación) son emitidas por el Identity Connector a través de zkSync (Capa 5) y solo los commitments batch llegan a Capa 1, lo que mantiene el costo de gas en un orden significativamente inferior al de Ethereum Mainnet directo.

Listado 1. Contrato inteligente de registro y revocación de Credenciales Verificables (fragmento).

```
pragma solidity ^0.8.20;
contract CredentialRegistry {
    mapping(address => bool) public isAuthorizedIssuer;
    mapping(bytes32 => bool) public isCredentialRevoked;
    event CredentialRegistered(bytes32 indexed credentialHash, address indexed
issuer);
    event CredentialRevoked(bytes32 indexed credentialHash, address indexed issuer);
    modifier onlyIssuer() {
        require(isAuthorizedIssuer[msg.sender], "Not an authorized issuer");
        _;}
    function registerCredentialHash(bytes32 credentialHash) external onlyIssuer {
        emit CredentialRegistered(credentialHash, msg.sender);  }
    function revokeCredential(bytes32 credentialHash) external onlyIssuer {
        isCredentialRevoked[credentialHash] = true;
        emit CredentialRevoked(credentialHash, msg.sender);}}
```

3.4 Flujo operativo: caso de uso de interconsulta

Para ilustrar el funcionamiento integrado de la arquitectura, se describe un caso de uso representativo de gestión de consentimiento informado para interconsulta. Un paciente acude a un prestador de salud externo (por ejemplo, una farmacia fuera de su red habitual) que necesita validar cobertura activa y acceder al resumen clínico (medicación actual y alergias) para realizar una dispensa segura. El flujo opera a través de las seis capas de la siguiente manera.

Autenticación (Capa 1 – Wallet/DID). El paciente se autentica mediante criptografía asimétrica desde su wallet digital, estableciendo una identidad auto-soberana sin credenciales centralizadas.

Emisión de la credencial (Capas 2, 3 y 4). El paciente genera un consentimiento digital estructurado como una VC con reglas granulares: qué efector accede (la farmacia), a qué segmento IPS-FHIR (alergias y medicación), y la duración del permiso. El Identity Connector, autenticado mediante SMART on FHIR, extrae los recursos FHIR pertinentes y construye la VC firmada con el DID institucional.

Anclaje de integridad (Capas 5 y 6). La credencial firmada se registra en zkSync (L2), publicando únicamente el hash criptográfico del consentimiento. Mediante ZK-SNARK, se genera una prueba matemática que permite a terceros verificar la validez y no-revocación del consentimiento sin acceder a su contenido. El ancla de confianza de Ethereum (L1) garantiza la inmutabilidad del registro raíz de emisores y del acumulador de revocaciones.

Validación y acceso (ciclo Verifier). La entidad validadora (obra social, farmacia o financiador) verifica la firma digital contra el registro en zkSync. Una vez validado el permiso criptográfico, el prestador receptor recibe acceso únicamente al paquete

IPS-FHIR autorizado. Si el paciente revoca el permiso desde su wallet, el acumulador en zkSync se actualiza y el acceso se invalida instantáneamente.

3.5 Escenarios de prueba

La validación técnica se aborda mediante la integración de microservicios contenerizados para interoperabilidad y terminologías, junto con componentes de gestión de identidad y acceso (OAuth 2.0/OpenID Connect). El entorno de pruebas se fundamenta en los componentes clínicos y de interoperabilidad provistos por la red RACSEL-LACPASS (RACSEL, s. f.). Se definen dos escenarios principales. El Escenario A (portabilidad del IPS y continuidad asistencial) verifica la emisión, presentación selectiva y actualización de datos clínicos en situaciones de movilidad regional, validando el ciclo completo Issuer–Holder–Verifier a través de las seis capas (HL7, s. f.a; HL7, s. f.b). El Escenario B (verificación de inmunizaciones con minimización de datos) evalúa el control criptográfico de autenticidad y no-revocación de certificados sanitarios —por ejemplo, Digital Vaccination Certificate (DVC) o International Certificate of Vaccination or Prophylaxis (ICVP)—, minimizando la exposición de datos del paciente mediante ZK-SNARKs y validando la viabilidad del modelo de costos en zkSync (Bai et al., 2022; Harrell et al., 2022; RACSEL, s. f.).

4 Resultados

Bajo el marco metodológico DSRM, se han completado las fases de identificación del problema, definición de objetivos y diseño/desarrollo del artefacto (Haryanti et al., 2022), y se han obtenido resultados preliminares de la fase de demostración. Los resultados materializados son dos: (i) la arquitectura de referencia de seis capas descrita en detalle en la Sección 3.2 e ilustrada en la Fig. 1, que garantiza privacidad por diseño (PHI off-chain) y escalabilidad operativa mediante la descomposición explícita de responsabilidades en capas especializadas; y (ii) el laboratorio de pruebas funcional y la evidencia técnica obtenida del despliegue, que se describen a continuación.

4.1 Laboratorio de pruebas funcional

Se desplegó un entorno reproducible basado en el IPS National Backend de RACSEL (RACSEL, s. f.) mediante infraestructura contenerizada (Docker Compose), habilitando pruebas funcionales de flujos IPS–FHIR e integración con perfiles IHE. El tiempo de despliegue completo del stack (primer levantamiento, incluyendo descarga de imágenes y carga inicial de terminologías) se mantuvo en el orden de decenas de minutos en hardware commodity, y los despliegues incrementales posteriores (sin descarga de imágenes) se completaron en pocos minutos, lo que confirma la viabilidad operativa del entorno para laboratorios académicos y proyectos piloto. El laboratorio integra los siguientes componentes. El núcleo clínico consiste en un servidor HAPI FHIR R4 con persistencia PostgreSQL, que implementa las operaciones CRUD sobre recursos clínicos y soporta la generación de bundles IPS (HL7, s. f.b). La capa semántica utiliza Snowstorm (SNOMED CT) sobre ElasticSearch para validación y normalización terminológica, asegurando la interoperabilidad semántica (RACSEL, s. f.). La mediación IHE se materializa en un IPS Mediator que soporta transacciones IHE MHD (ITI-65/66/67/68) sobre bundles

IPS, habilitando la publicación, búsqueda y recuperación de documentos clínicos conforme a los perfiles de integración (IHE, s. f.b; RACSEL, s. f.). Los servicios de firma y verificación incluyen firma digital, transformaciones IPS→DVC/ICVP y generación de Enlaces de Salud Verificables (VHL), que permiten la verificación de integridad y autenticidad de los documentos clínicos intercambiados (RACSEL, s. f.). Este laboratorio constituye la base técnica para la ejecución de los escenarios de prueba descritos en la Sección 3.5 y para la integración de los componentes SSI y blockchain (Capas 3 a 6 de la arquitectura).

4.2 Evidencia técnica: Credencial Verificable y viabilidad de costos

Para aportar evidencia técnica concreta del artefacto, se presenta un fragmento de la estructura de una Credencial Verificable emitida por el Identity Connector, en la que se incluye un apuntador al recurso FHIR subyacente sin publicar datos clínicos on-chain (Listado 2).

Listado 2. Fragmento de Credencial Verificable (VC) que enlaza a un recurso FHIR Immunization y cuyo hash se ancla en zkSync.

```
{  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vaccination/v1"],
  "id": "urn:uuid:8c71e67e-2d11-4e8e-9bfc-2a2e0a28e4c1",
  "type": ["VerifiableCredential", "ImmunizationCredential"],
  "issuer": "did:ethr:zksync:0x8f9...c1a",
  "issuanceDate": "2026-04-10T14:32:18Z",
  "credentialSubject": {
    "id": "did:key:z6MkpTHR8...gK",
    "fhirReference": {
      "resourceType": "Immunization",
      "url": "https://fhir.lab.example/Immunization/987",
      "sha256": "b3a1...f7e2"}},
  "credentialStatus": {
    "id": "did:ethr:zksync:0x8f9...c1a#rev-accumulator",
    "type": "RSAAccumulator2023"},
  "proof": { "type": "Ed25519Signature2020", "proofValue": "z58..." }}
```

El bundle IPS generado por HAPI FHIR durante las pruebas presentó un payload con tamaños del orden de unas decenas de kilobytes para un paciente con historial clínico representativo (incluyendo secciones de alergias, medicación e inmunizaciones), lo que resulta compatible con su transporte a través de perfiles IHE MHD en redes móviles. Respecto del costo transaccional, el uso de zkSync (L2) permite registrar el hash de cada VC y las actualizaciones del acumulador de revocaciones a un costo esperado de entre uno y dos órdenes de magnitud inferior al equivalente directo en Ethereum Mainnet, según las estimaciones públicas reportadas para ZK-rollups (Matter Labs, s. f.). Esta estimación teórica respalda la viabilidad económica de la arquitectura para escenarios con un volumen alto de emisiones, verificaciones y revocaciones; la medición empírica sobre el prototipo integrado queda comprendida dentro de la fase de evaluación de DSRM.

5 Discusión

La arquitectura de seis capas propuesta es técnicamente viable y permite articular un flujo de intercambio clínico donde el paciente retiene el control soberano de sus datos. La descomposición especializada —frente a las tres capas genéricas del modelo Issuer–Holder–Verifier— ofrece una separación más granular de responsabilidades

que facilita tanto la validación independiente de cada componente como la evolución modular del sistema. Este enfoque contrasta con los trabajos de de Siqueira et al. (2021), Bai et al. (2022) y Harrell et al. (2022), que si bien abordan SSI en salud, no integran de forma explícita perfiles IHE ni abordan la operacionalización del IPS dentro de un entorno de laboratorio reproducible. La inclusión de PDQm, MHD y SVCM resuelve brechas de interoperabilidad técnica y semántica que la literatura previa no había abordado sistemáticamente en conjunción con SSI, y la incorporación del Identity Connector como puente bidireccional entre sistemas legados EHR/FHIR y el ecosistema SSI es un aporte diferenciador, dado que la mayoría de las propuestas previas asumen entornos nativos SSI sin considerar la integración con infraestructura clínica existente.

La inclusión de ZK-SNARKs en la capa SSI responde a una necesidad crítica identificada en el caso de uso de interconsulta: la validación de afirmaciones —validez del consentimiento, autenticidad de la credencial y no-revocación— sin exposición de información clínica subyacente (Sasson et al., 2014). Este mecanismo, combinado con la ejecución en zkSync (L2), indica un camino promisorio para mitigar los costos transaccionales de Ethereum (L1), aspecto crítico para escenarios con alto volumen de emisiones y verificaciones. Adicionalmente, el uso de acumuladores criptográficos para la gestión de la revocación, en lugar de listas estáticas de hashes revocados, fortalece la compatibilidad con el principio de minimización de datos de GDPR, dado que habilita pruebas de no-pertenencia sin publicar un listado persistente de credenciales revocadas que pudiera actuar como identificador indirecto.

El laboratorio desplegado sobre el stack RACSEL–IPS National Backend (RACSEL, s. f.) proporciona un entorno reproducible y contenerizado para la ejecución de escenarios de portabilidad del IPS y verificación de inmunizaciones, y constituye la base técnica para la demostración extremo a extremo del prototipo en las fases subsiguientes de DSRM. Entre las limitaciones del estudio se encuentran, en primer lugar, la ausencia aún de resultados empíricos de rendimiento sobre la infraestructura L1/L2 integrada con los componentes clínicos; en segundo lugar, la necesidad de validar el modelo de consentimiento granular con usuarios reales en escenarios clínicos; y, en tercer lugar, la dependencia del entorno de pruebas de componentes específicos de RACSEL cuya generalizabilidad debe ser evaluada en contextos diversos. Un desafío adicional, que la literatura sobre SSI identifica como la principal barrera para la adopción masiva, es la usabilidad de la wallet por parte de pacientes reales: la gestión y custodia de claves privadas, la recuperación de wallets en caso de pérdida del dispositivo y el soporte para usuarios con bajas competencias digitales son dimensiones que exceden el alcance técnico del presente artefacto y requieren, para su abordaje, esquemas de recuperación social (social recovery) y experiencias de usuario específicamente diseñadas. Otro aspecto crítico para la adopción masiva de la solución propuesta es la necesidad de establecer mecanismos de gobernanza interinstitucional que definan con claridad roles, responsabilidades y criterios de confianza entre efectores, financiadores, organismos públicos y proveedores tecnológicos. En escenarios reales, la viabilidad técnica de una arquitectura interoperable no garantiza por sí sola su incorporación efectiva al sistema de salud: resulta necesario acordar quiénes pueden actuar como emisores autorizados,

bajo qué procedimientos se auditan las credenciales, cómo se resuelven disputas sobre datos incorrectos o desactualizados, y qué incentivos operativos justifican la integración de sistemas heterogéneos ya existentes. Por ello, además de la validación técnica del prototipo, la adopción a escala requiere marcos de gobernanza, acuerdos normativos y modelos de responsabilidad compartida que permitan trasladar la arquitectura desde un entorno controlado de laboratorio hacia redes sanitarias reales, diversas y reguladas.

En las fases subsiguientes de DSRM (demostración y evaluación), se prevé obtener evidencia empírica mediante la ejecución de un prototipo integrado extremo a extremo que cubra el ciclo Issuer–Holder–Verifier a través de las seis capas (Haryanti et al., 2022). Los resultados esperados incluyen la validación técnica de integridad criptográfica y verificación de estado de no-revocación sobre infraestructura L1/L2 (Ethereum, s. f.; Matter Labs, s. f.); métricas de desempeño —latencia, tasas de éxito en emisión y verificación, y costo por operación en zkSync—; y escenarios de movilidad que validen funcionalmente la portabilidad del IPS y la verificación de certificados sanitarios con minimización de datos (Bai et al., 2022; Harrell et al., 2022).

6 Conclusiones y Trabajos Futuros

Este trabajo presenta una arquitectura de seis capas para el intercambio interjurisdiccional de información clínica basada en Identidad Auto-Soberana (SSI). La arquitectura integra estándares W3C (DIDs/VCs) con HL7 FHIR, el International Patient Summary (IPS) y perfiles IHE (PDQm, MHD, SVCM), e incorpora pruebas de conocimiento cero (ZK-SNARKs) para la validación de afirmaciones sin exposición de datos clínicos. El marco de confianza se ancla en Ethereum (L1) con operaciones eficientes en zkSync (L2), preservando la privacidad del paciente mediante un diseño que mantiene la información clínica protegida fuera de la cadena y utiliza acumuladores criptográficos para la gestión de la revocación.

Las contribuciones principales del estudio son: la definición de una arquitectura de seis capas que descompone explícitamente las responsabilidades de soberanía del paciente, interoperabilidad clínica, integración de sistemas legados, identidad descentralizada con ZK-Proofs, ejecución eficiente en L2 y anclaje de confianza en L1; la introducción del componente Identity Connector como puente bidireccional entre sistemas legados EHR/FHIR y el ecosistema SSI, apoyado en SMART on FHIR y mapeo de identificadores a DIDs; la especificación del contrato inteligente de registro y revocación de credenciales, con semántica explícita del rol de zkSync como capa de ejecución para operaciones de identidad; y el despliegue de un laboratorio de pruebas reproducible basado en el stack contenerizado RACSEL–IPS National Backend que habilita la validación funcional de flujos IPS–FHIR con perfiles IHE.

Como trabajos futuros concretos, se prevé completar las fases de demostración y evaluación de DSRM mediante la ejecución del prototipo integrado extremo a extremo sobre el ciclo Issuer–Holder–Verifier a través de las seis capas de la arquitectura. Específicamente, se llevarán a cabo las siguientes líneas de trabajo: validación empírica de la integridad criptográfica y de la verificación de estado de no-revocación sobre infraestructura L1/L2; medición de métricas de desempeño (latencia, tasas de éxito y costo por operación en zkSync, con comparación directa

contra Ethereum Mainnet); ejecución de escenarios de movilidad regional para portabilidad del IPS y verificación de certificados sanitarios con minimización de datos; evaluación del modelo de consentimiento granular con usuarios reales en entornos clínicos simulados, con foco específico en la usabilidad de la wallet, esquemas de social recovery y soporte para la diversidad de perfiles de paciente; y exploración de la integración de esquemas de cifrado totalmente homomórfico (FHE) que permitan la ejecución de análisis automatizados sobre datos clínicos cifrados sin comprometer la confidencialidad del paciente.

Referencias

Bai, P., Kumar, S., Aggarwal, G., Mahmud, M., Kaiwartya, O. y Lloret, J. (2022). Self-sovereignty identity management model for smart healthcare system. Sensors, 22(12), 4714. https://doi.org/10.3390/s22124714

de Siqueira, A. G., da Conceição, A. F. y Rocha, V. (2021). User-centric health data using self-sovereign identities. arXiv. https://doi.org/10.48550/arXiv.2107.13986

Ethereum. (s. f.). Introduction to Ethereum. https://ethereum.org/en/what-is-ethereum/

Harrell, D. T., Usman, M., Hanson, L., Abdul-Moheeth, M., Desai, I., Shriram, J. … Khurshid, A. (2022). Technical design and development of a self-sovereign identity management platform for patient-centric healthcare using blockchain technology. Blockchain in Healthcare Today, 5, 196. https://blockchainhealthcaretoday.com/index.php/journal/article/view/196

Haryanti, T., Rakhmawati, N. A., Subriadi, A. P. y Tjahyanto, A. (2022). The Design Science Research Methodology (DSRM) for Self-Assessing Digital Transformation Maturity Index in Indonesia. 2022 IEEE 7th International Conference on Information Technology and Digital Applications (ICITDA), 1–7. https://doi.org/10.1109/ICITDA55840.2022.9971171

HL7. (s. f.a). HL7 FHIR: International Patient Summary (IPS) Implementation Guide. https://hl7.org/fhir/uv/ips/

HL7. (s. f.b). FHIR Release 4 (R4) Specification. https://hl7.org/fhir/R4/

IHE. (s. f.a). Patient Demographics Query for Mobile (PDQm). https://profiles.ihe.net/ITI/PDQm/

IHE. (s. f.b). Mobile Access to Health Documents (MHD). https://profiles.ihe.net/ITI/MHD/

IHE. (s. f.c). Sharing Valuesets, Codes, and Maps (SVCM). https://profiles.ihe.net/ITI/SVCM/

Matter Labs. (s. f.). zkSync Documentation. https://docs.zksync.io

RACSEL. (s. f.). Red de América Latina y el Caribe de Cooperación en Salud Digital (RACSEL-LACPASS). https://github.com/RACSEL/

Salah, D., Mnasri, S. e Idoudi, H. (2025). Self-Sovereign digital identity in blockchain-based systems for e-health cards management. Procedia Computer Science, 270, 985–993. https://doi.org/10.1016/j.procs.2025.09.219

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. y Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. 2014 IEEE Symposium on Security and Privacy, 459–474. https://doi.org/10.1109/SP.2014.36

W3C. (2022a). Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations. W3C Recommendation. https://www.w3.org/TR/did-core/

W3C. (2022b). Verifiable Credentials Data Model v1.1. W3C Recommendation. https://www.w3.org/TR/vc-data-model/