ugr | Universidad de Granada

TRABAJO FIN DE GRADO

INGENIERÍA INFORMÁTICA

Implementación en Android de un agente de Identidad auto-Soberana (SSI) utilizando Hyperledger Aries

Autor
Iván Cortón da Silva

Director
Rafael Alejandro Rodríguez Gómez

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE TELECOMUNICACIÓN

DEPARTAMENTO DE TEORÍA DE LA SEÑAL, TELEMÁTICA Y COMUNICACIONES

ÍNDICE

DE PROFESIONALES TI IDENTIFICAN LA SEGURIDAD COMO PRINCIPAL DESAFIO EN LA GESTIÓN DE REDES*

*** Según el Global Networking Trends de Cisco, 2023**

MOTIVACIÓN

Crecimiento exponencial de Internet -> Aumento masivo de comunicaciones

Regulaciones existentes y métodos de autenticación -> Desconfianza

Oportunidad de Innovación -> Necesidad de enfrentar desafíos de identificación en línea

BLOCKCHAIN

Tecnología de almacenamiento de datos que utiliza una lista de registros enlazados llamados bloques

Hyperledger es un proyecto único de *blockchain* centrado en la identidad en lugar de cambio de activos

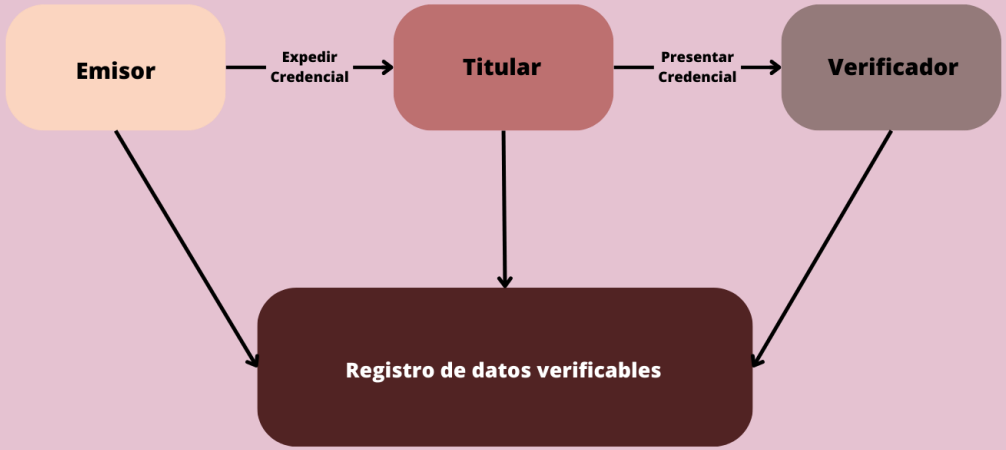
Cuatro elementos registrados en la *blockchain* de Hyperledger

IDENTIDAD AUTO-SOBERANA (SSI)

Control Total de tu Identidad

Facilita la Verificación de Credenciales

Adiós a las Contraseñas Olvidadas



PROYECTO HYPERLEDGER

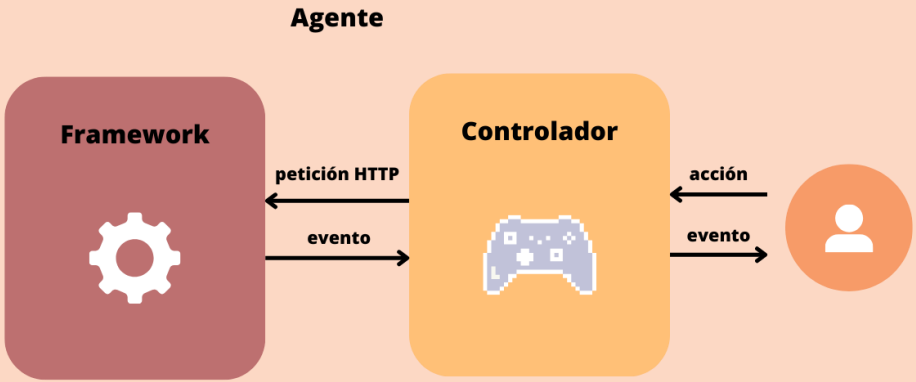
INDY	Creación de una infraestructura de identidad digital descentralizada y autónoma. Facilita la gestión segura de identidades digitales y su verificación. Nodos Indy
ARIES	Herramientas y protocolos que permiten el intercambio seguro de datos de identidad. Aries extiende las capacidades de Indy y proporciona una base sólida para la creación de aplicaciones de identidad descentralizada.
URSA	Se enfoca en la criptografía y la seguridad. Proporciona una biblioteca común y modular de criptografía que puede ser utilizada por otros proyectos de Hyperledger

ESTADO DEL ARTE

	FUNCIONAL	FACILIDAD	DESCARGAS	PLATAFORMA	GRATIS
Trinsic Wallet	CONEXIONES ✓ CREDENCIALES ✓	✓	1K+	ANDROID E IOS	✗
IdRamp Cello	CONEXIONES ✓ CREDENCIALES ✓	✗	50+	ANDROID E IOS	✓
Connect.Me	CONEXIONES ✓ CREDENCIALES ✗	✓	10K+	ANDROID E IOS	✓
iGrant.io	CONEXIONES ✓ CREDENCIALES ✗	✗	1K+	ANDROID E IOS	✓

OBJETIVO GENERAL

Desarrollo de una aplicación Android que integre el ecosistema ARIES para la gestión de credenciales, permitiendo generar, almacenar y operar tanto como emisor como titular de credenciales.



OBJETIVOS ESPECÍFICOS

Estudio del ecosistema ARIES y proyecto Hyperledger de la *Linux Foundation*

⬇

Diseño e implementación de una aplicación Android

⬇

Integración de la tecnología ARIES a través de *framework* con red INDY local

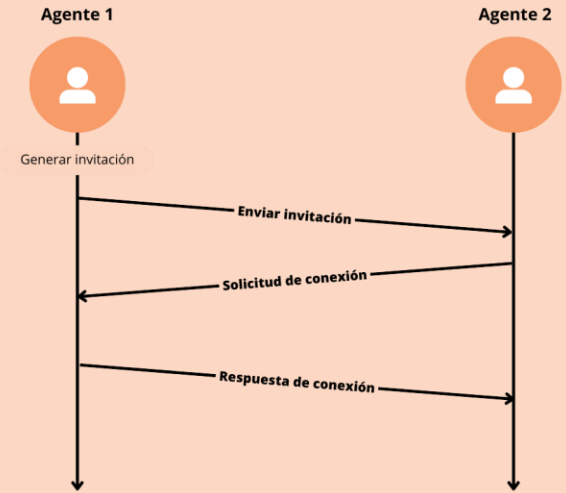
⬇

Pruebas sobre el correcto funcionamiento de la aplicación

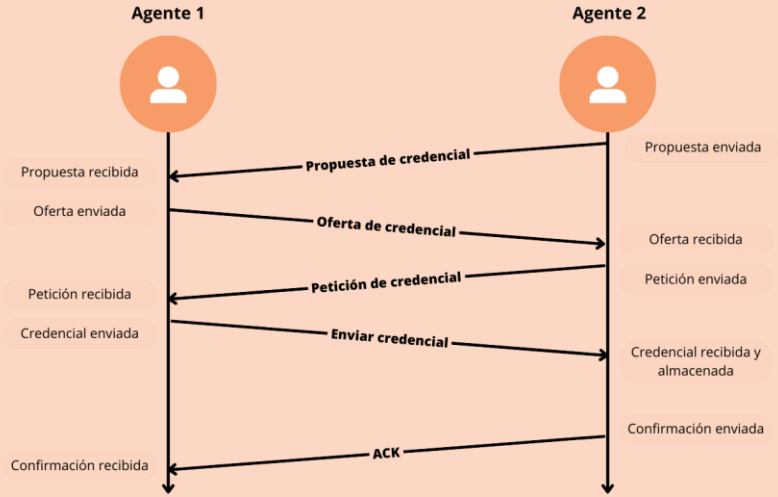
Emisor genera un esquema de credenciales válido

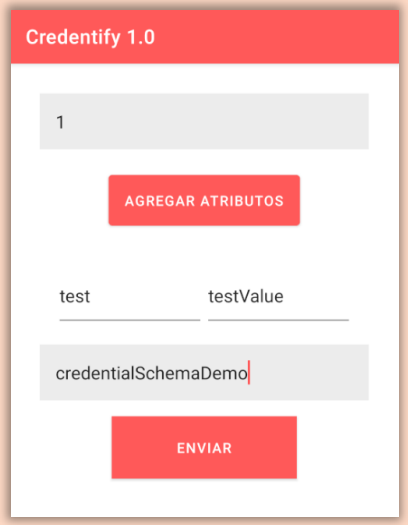
Registro exitoso en nuestra cartera

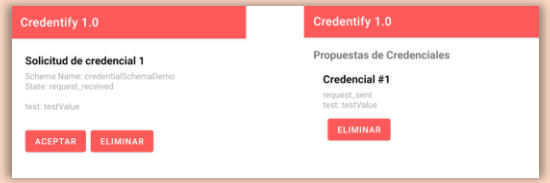
CASOS DE USO DE LA APLICACIÓN

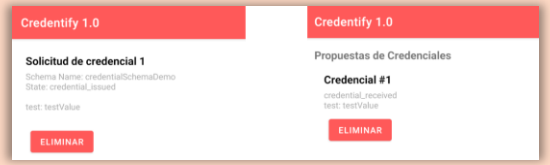


CASOS DE USO DE LA APLICACIÓN









CASOS DE USO DE LA APLICACIÓN

Demostración

IVÁN CORTÓN DA SILVA

CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

Logros destacados

Investigación en profundidad de Identidad auto-Soberana: Proyectos Hyperledger

Desarrollo de controladores para interactuar como agentes ARIES

Implementación de entorno completo con red local y uso de *framework*

Eficiencia en el uso de recursos para el despliegue

CONCLUSIONES Y LÍNEAS DE TRABAJO FUTURAS

Líneas de trabajo futuras

Desarrollo de un manual completo de uso, configuración y resolución de problemas

Ampliación de la variedad de casos de uso

Pruebas de eficiencia y estudio del rendimiento de la solución

Adaptación y extensión a dispositivos iOS

GRACIAS POR SU TIEMPO Y ATENCIÓN

IVÁN CORTÓN DA SILVA