



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

- Motivación
- Blockchain
- ¿Qué es una Identidad auto-Soberana?
- Proyecto Hyperledger
- Estado del Arte
- Objetivos
 - Objetivo general
 - Objetivos específicos
- Casos de Uso
- Conclusiones y Líneas de Trabajo Futuras



**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)



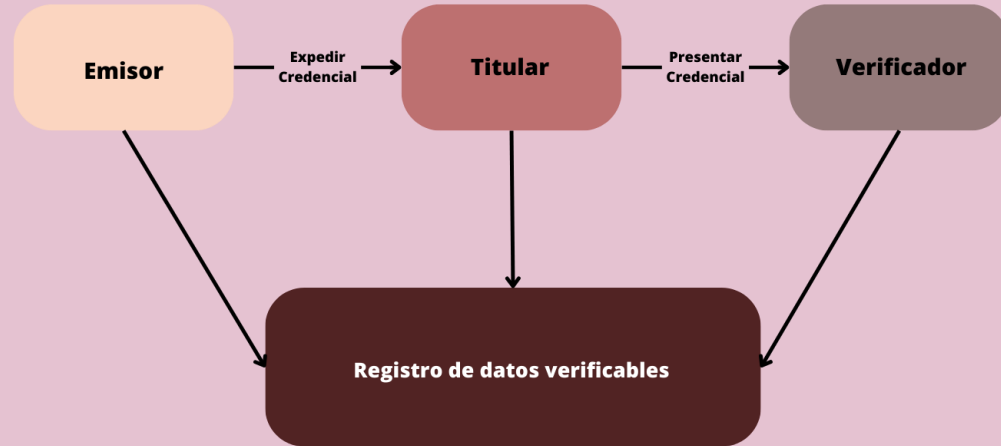
Control Total de tu Identidad



**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.

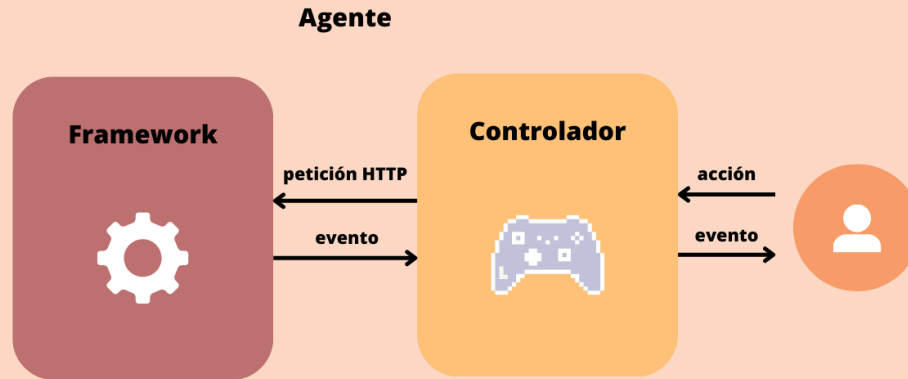
URSA

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

	FUNCIONAL	FACILIDAD	DESCARGAS	PLATAFORMA	GRATIS
Trinsic Wallet	<div>CONEXIONES</div> <div>CREDENCIALES</div> <div>✓</div> <div>✓</div>	✓	1K+	ANDROID E IOS	✗
IdRamp Cello	<div>CONEXIONES</div> <div>CREDENCIALES</div> <div>✓</div> <div>✓</div>	✗	50+	ANDROID E IOS	✓
Connect.Me	<div>CONEXIONES</div> <div>CREDENCIALES</div> <div>✓</div> <div>✗</div>	✓	10K+	ANDROID E IOS	✓
iGrant.io	<div>CONEXIONES</div> <div>CREDENCIALES</div> <div>✓</div> <div>✗</div>	✗	1K+	ANDROID E IOS	✓
		ESTADO DEL ARTE			
					10

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

Credentify 1.0

1

AGREGAR ATRIBUTOS

testValueSchema00

testNewSchema00

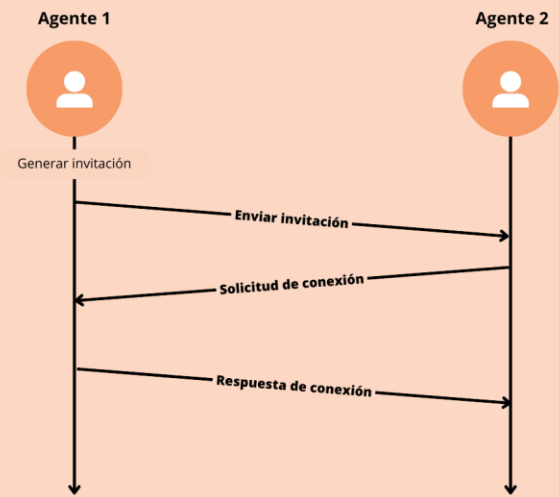
Credential Definition ID:
WPh2Xz3e4Sgu2vwjGq5HZ5:3:CL:
400:testNewSchema00

ENVIAR

Emisor genera un esquema de credenciales válido

Registro exitoso en nuestra cartera

CASOS DE USO DE LA APLICACIÓN



Credentify 1.0

CREAR CREDENTIAL SCHEMA

GESTIONAR CREDENCIALES

CREAR INVITACIÓN DE CONEXIÓN

Invitación

```
{ "@type": "did:sov:
BzCbsNYhMrjHiqZDTUASHg:spec\
/connectionsV1.0/invitation"
, "@id": "99debb14-f80b-4100-9217
-4640bd96f43b", "label": "Issuer"
, "serviceEndpoint": "http://host
.docker.internal:8000", "recipientKeys":
```



Credentify 1.0

DESCONECTADO

ENVIAR PROPUESTA SCHEMA

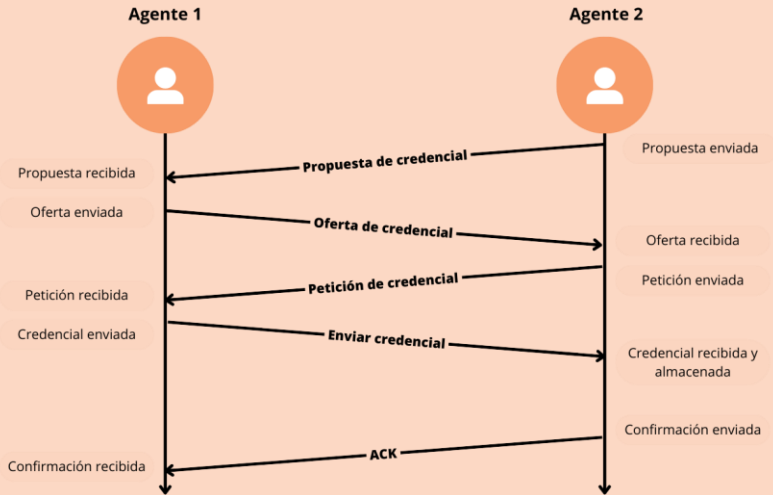
GESTIONAR CREDENCIALES

ACEPTAR INVITACIÓN

3J3WJfAtYfhqqD8vdaPwMmPPU6X"]]

```
{ "accept": "auto", "invitation_mode": "once",
"rfc23_state": "request-sent", "created_at":
"2023-09-02 12:10:59.737168Z",
"invitation_key": "8fAu4VqZtBgxTfKGd
3J3WJfAtYfhqqD8vdaPwMmPPU6X",
"updated_at": "2023-09-02 12:10:59.843711Z",
"their_role": "inviter", "connection_id":
"60a593ba-669b-405b-ad8f-52adb463bff2",
"mv_did": "FRrVtfvSSkl Disn8iel FaA"
```

CASOS DE USO DE LA APLICACIÓN



Credentify 1.0

1

AGREGAR ATRIBUTOS

test testValue

credentialSchemaDemo

ENVIAR

Credentify 1.0

Credentify 1.0

Solicitud de credencial 1

Schema Name: credentialSchemaDemo

State: request_received

test: testValue

ACEPTAR

ELIMINAR

Propuestas de Credenciales

Credencial #1

request_sent

test: testValue

ELIMINAR

Credentify 1.0

Credentify 1.0

Solicitud de credencial 1

Schema Name: credentialSchemaDemo

State: credential_issued

test: testValue

ELIMINAR

Propuestas de Credenciales

Credencial #1

credential_received

test: testValue

ELIMINAR

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