Universidad Politécnica

de Madrid

Escuela Técnica Superior de

Ingenieros Informáticos

Grado en Ingeniería Informática

Trabajo Fin de Grado

Evaluación de compatibilidad de modelos y marcos de identidad digital

Autor: Víctor Carrión Martín

Tutor(a): Francisco Javier Soriano Camino

Cotutor: Juan Luis Gozalo Fernández

Madrid, Febrero de 2024

Plan de trabajo

Grado en Ingeniería Informática

Título: Análisis y evaluación de modelos y marcos de identidad digital

Febrero 2024

Autor: Víctor Carrión Martín

Tutor:

Francisco Javier Soriano Camino

Departamento de Lenguajes y Sistemas Informáticos e Ingeniería de Software

ETSI Informáticos

Universidad Politécnica de Madrid

Cotutor:

Juan Luis Gozalo Fernández

Blockchain Delivery Manager

Inetum

Agradecimientos

Quiero agradecer a mi tutor Javier Soriano por la orientación proporcionada, que me ha ayudado a darle forma a mi trabajo. También, a mi cotutor Juan Luis, Blockchain Delivery Manager de Inetum, por toda la atención recibida durante el desarrollo del trabajo.

Muchas gracias a los profesores que me han aportado valor durante la carrera, haciendo una especial mención a Alfonso Zamora, Francisco Rosales, Guillermo Vigueras, Guillermo Román, María Luisa Córdoba y Víctor Robles

También muchas gracias por la impagable ayuda de los compañeros que me han acompañado durante estos años, que más que compañeros, son amigos y algunos muy amig@s.

Finalmente, quiero agradecerle a mi familia por todo, gracias a mis padres por el apoyo, y por la forma en la que me han educado, ya que gracias a esa educación estoy donde estoy. Gracias a mis hermanos y a mi novia, quien ha sido un apoyo fundamental en este proceso.

GRACIAS

Resumen

La identidad digital es la forma en que todos nos identificamos dentro de nuestras interacciones en línea, que ahora representan una gran parte de nuestras interacciones diarias. Dentro de los estilos de identidad digital, la identidad digital autogestionada (SSI, del inglés Self-Sovereign Identity), es un nuevo modelo de gestión de la identidad digital que representa una innovación radical en este campo. Son numerosos los modelos de identidad digital desarrollados hasta la fecha. Este trabajo plantea el estudio y análisis comparativo de los principales modelos existentes, centrándose en los basados en SSI. A partir de este análisis, se profundizará en la compatibilidad existente entre dos de estos modelos: el modelo de identidad digital de Alastria (AlastriaID) y el modelo de la Unión Europea (EUDI). Finalmente, se realizará una pequeña prueba de concepto para trasladar los conocimientos teóricos vistos en la investigación sobre la creación de credenciales, emisión de credenciales, aprobación de credenciales, etc.

Abstract

Digital identity is the way we all identify ourselves within our online interactions, which now represent a large part of our daily interactions. Within digital identity styles, Self-Sovereign Identity (SSI) is a new digital identity management model that represents a radical innovation in the field. Numerous digital identity models have been developed to date. This paper proposes the study and comparative analysis of the main existing models, focusing on those based on SSI. From this analysis, the compatibility between two of these models will be studied: Alastria's digital identity model (AlastriaID) and the European Union's model (EUDI). Finally, a small proof of concept test will be conducted to transfer the theoretical knowledge seen in the research on credential creation, credential issuance, credential approval, etc.

Tabla de contenidos

Índice de figuras

Acrónimos

AP+. *Australian Payments Plus*
API. *Application Programming Interface*
AUII. *Autoridad Única de Identificación de India*

BID Lab. *Laboratorio del Grupo Banco Interamericano de Desarrollo*

CNUDMI. *Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Comisión de las Naciones Unidas para el Derecho Mercantil Internacional*
CPF. *Cadastro de Pessoas Físicas*
CPQD. *Centro de Pesquisa e Desenvolvimento em Telecomunicações*
CSP. *Credential Solution Provider*
CURP. *Clave Única de Registro de Población*

DGB. *Digital Government Blueprint*
DID. *Descentralized Identifiers*
DLT. *Distributed Ledger Technology*
DNI. *Documento Nacional de Identidad*
DPDP. *Digital Personal Data Protection Bill*
DPI. *Digital Public Infraestructure*

EBP. *European Blockchain Partnership*
EBSI. *European Blockchain Services Infraestructure*
EDIW. *EUDI Wallet*
eIDAS. *electronic IDentification, Authentication and trust Services*
EUDI. *Identidad Digital de la Unión Europea*
EVM. *Ethereum VirtualMachine*

GAFI. *Grupo de Acción Financiera Internacional, Grupo de Acción Financiera Internacional*

ICN. *Identificação Civil Nacional*

IdP. *ID Provider*

LGPD. *Lei Geral de Proteção de Dados*

MeitY. *Ministerio de Electrónica y Tecnología de la Información*
MFA. *Multi Factor Authentication*
MinTIC. *Ministerio de Tecnologías de la Información y las Comunicaciones*

NIST. *National Institute of Standards and Technology*

OID4VC. *OpenID para VC*
OID4VCI. *OpenID for Verifiable Credential Issuance*
OID4VP. *OpenID for Verifiable Presentations*

PCTF. *Pan-Canadian Trust Framework*
PID. *Personally Identifiable Data*
PKI. *Public Key Infraestructure*
PNB. *National Blockchain Project*
PoA. *Proof of Authority*
PYME. *microempresas, pequeñas y medianas empresas*

RGPD. *Reglamento General de Protección de Datos*
RMF. *Risk Management Framework*
RP. *Reliying Parites*

SFC. *Superintendencia Financiera de Colombia*
SGTS. *Singapore Government Technology Stack*
SID. *Sistmea de Identidad Digital*
SSI. *Self-Sovereign Identity*

TDIF. *Trusted Digital Identity Framework*
ToIP. *Trust over IP*

VC. *Verifiable Credential*

1 Introducción

El objetivo de este trabajo es realizar un estudio global sobre la identidad digital y el modelo de identidad digital autogestionada, estudiando la situación en distintos países del mundo, e investigando distintos modelos existentes. Luego se continuará con una comparativa de dos modelos principales, el español Alastria[1] ID y el europeo EBSI[2] (European Blockchain Services Infrastructure).

1.1 Contexto

1.1.1 Identidad Digital

El primer paso para abordar este trabajo es entender brevemente qué es la identidad digital (en inglés Digital Identity). La identidad digital es el conjunto de datos e información que permite identificar y/o autentificar a una persona, organización, dispositivo… en el mundo digital o en la red. También se define como "representación única de un sujeto que realiza una transacción en línea". (Grassi et al., 2017a)

1.1.2 Self-Sovereign Identity

Self-Sovereign Identity [3] (SSI), al español, identidad autogestionada o autosoberana, es un nuevo modelo de identidad digital en internet. En este modelo, tanto individuos como organizaciones tienen autonomía total sobre su identidad y la gestionan por sí mismos. Esto significa que tienen la capacidad de gestionar sus credenciales de identidad por su cuenta y utilizarlas de forma más privada según lo necesiten. En el sistema de identidad autogestionada, la capacidad para controlar quién accede a qué información es fundamental. Lo que convierte a la privacidad en una propiedad principal de su arquitectura.

En resumen, la identidad autogestionada es un enfoque que otorga a individuos y organizaciones el poder de manejar su propia identidad digital de forma segura y privada. Esto les permite establecer relaciones de confianza con mayor eficacia y proteger su información personal.

---

[1] https://alastria.io/que-es-alastria/
[2] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home
[3] https://www.dock.io/post/self-sovereign-identity#introduction

1.1.3 Blockchain

"Una blockchain[4] no es otra cosa que una base de datos que se halla distribuida entre diferentes participantes, protegida criptográficamente y organizada en bloques de transacciones relacionados entre sí matemáticamente" (Alexander Preukschat, 2017). La integridad de los datos se garantiza mediante este sistema descentralizado, permitiendo a partes no del todo confiables llegar a un consenso sobre la existencia, el estado y la evolución de información compartida. En la blockchain, la confianza y el consenso son factores fundamentales que permiten generar confianza en la información almacenada por todos los participantes.

La blockchain se construye técnicamente a través de una red global de ordenadores/nodos que gestionan una enorme base de datos. Se puede hacer pública esta base de datos, abierta a todos los participantes, o privada y restringida solo a unos pocos. La primera blockchain pública que se lanzó fue la de Bitcoin en 2009. La tecnología blockchain se fundamenta en un sistema de registro distribuido, donde cada nodo de la red tiene una copia idéntica de la cadena de bloques, lo que garantiza la descentralización y seguridad de los datos.

Por lo tanto, podríamos decir que una blockchain es un sistema descentralizado e inalterable para el registro de transacciones, en el que la confianza y el consenso se alcanzan mediante una red interconectada de nodos que validan y registran las transacciones de forma segura y transparente.

1.2 Objetivos

Los principales objetivos de este trabajo son los siguientes:

1. Estudio sobre la identidad digital y el modelo self-sovereign identity
2. Estudio de las características de los principales modelos y marcos de identidad digital existentes
3. Análisis comparativo de los modelos de identidad digital considerados
4. Análisis de compatibilidad de los modelos de identidad digital de

[4] https://www.ibm.com/topics/blockchain

Alastria (AlastriaID) y de la Unión Europea (EUDI[5])

5. Prueba de concepto de identidad digital.

1.3 Plan de trabajo

1. Estudio de la identidad digital.

2. Estudio sobre el modelo de identidad digital "self-sovereign identity"

3. Análisis del estado del arte en modelos y marcos de identidad digital. Identificación de los principales modelos y marcos, descripción, principales características.

4. Estudio modelos internacionales.

5. Análisis comparativo de los principales modelos y marcos de identidad digital.

6. Análisis de compatibilidad entre AlastriaID y EUDI.

7. Redacción de un documento de memoria de TFG.

8. Elaboración de material de apoyo para la defensa del TFG

9. Prueba de concepto de identidad digital.

Tareas	15-29 Feb	1-15 Marzo	15-31 Marzo	1-15 Abril	15-30 Abril	1-15 Mayo	15-31 Mayo	1-3 Junio
Tarea 1								
Tarea 2								
Tarea 3								
Tarea 4								
Tarea 5								
Tarea 6								
Tarea 7								
Tarea 8								
Tarea 9								

[5] https://github.com/eu-digital-identity-wallet

2 Estado del arte

2.1 SSI: Principios y fundamentos

Como hemos visto, la identidad autogestionada (SSI) es un nuevo modelo de identidad digital cuyo principal objetivo es demostrar quiénes somos (como persona, organización…) ante sitios web, servicios, aplicaciones…etc.

A pesar de la importancia de la adopción de SSI, en un evento de 2019 llamado "The Future of Digital Identity," organizado por Vinod Baya, director y jefe de "Emerging Technology at Citi Ventures Inc.", señaló que existen tres desafíos principales para esta adopción:

- Construir un nuevo ecosistema SSI.
- Gestión descentralizada de claves.
- Acceso offline (sin internet).

2.1.1 Componentes centrales de la arquitectura SSI

A continuación, vamos a ver siete componentes básicos[6] de SSI.

2.1.1.1 Credenciales Verificables (VC)

Para empezar, con el término credencial nos referimos a los documentos que podemos llevar en nuestra cartera (o no) para demostrar nuestra identidad. Por ejemplo: tarjeta de crédito, permiso de conducir, tarjetas de empleo…

Desde una perspectiva técnica las "credenciales" son cualquier conjunto de información protegida contra alteraciones o intentos no autorizados de modificación, que una autoridad declara como verídica sobre el sujeto por una autoridad. Las credenciales verificables permiten a la persona que las poseen influir en la confianza de otras personas sobre si las afirmaciones son verdaderas o no. La credencial se emite por una autoridad confiable, lo que garantiza la confianza en ella. Por ejemplo:

---

[6] Preukschat, A., Reed, D., Allen, C., & Vogelsteller, F. (2021b). *Self-Sovereign Identity Chapter 1 Why the internet is missing an identity layer—and why SSI can finally provide one.*

- Un diploma expedido por una universidad demuestra que tienes un título educativo.
- Una factura de servicios públicos demuestra que usted es un cliente registrado de la empresa de servicios públicos que emitió la factura.

Una vez aclarado esto, las credenciales verificables son el equivalente digital a las credenciales físicas explicadas previamente. Las VC's deben ser verificables, es decir, que los verificadores deben tener la capacidad de determinar quién emitió la credencial, si ha sido alterada y si está vigente. Para lograrlo, se usa la criptografía de clave pública/privada. La persona que posee la credencial utiliza su clave privada para firmar digitalmente dicha credencial, y los verificadores pueden verificar la autenticidad de la firma utilizando la correspondiente clave pública.

2.1.1.2 Emisores, titulares y verificadores

- Los emisores son las entidades responsables de emitir las credenciales, estas pueden ser emitidas por individuos u organizaciones como agencias gubernamentales, instituciones financieras o universidades.
- Las personas u organizaciones que solicitan y poseen las credenciales son los titulares. Los titulares piden a los emisores sus credenciales, las guardan en su billetera digital y muestran pruebas de las afirmaciones de una o más credenciales cuando los verificadores lo solicitan. Los titulares pueden ser tanto individuos como organizaciones que usen billeteras empresariales.
- Los verificadores son aquellos que buscan validar la información contenida en las credenciales, y asegurarse de la autenticidad de la persona, organización o entidad que se presenta como titular de la credencial. Los verificadores solicitan una o más afirmaciones de una o varias VC's, sobre los titulares, para presentar pruebas. Si el titular está de acuerdo, su agente proporcionará una prueba que el verificador puede confirmar. La verificación de la firma digital del emisor, que generalmente se realiza con un Identificador Descentralizado (DID), es el paso crítico en este proceso, que garantiza la autenticidad de la credencial y genera confianza en la entidad emisora.

2.1.1.3 Carteras digitales

Las carteras digitales son como las carteras físicas, con la diferencia de que permiten almacenar y gestionar credenciales verificables. Estas carteras deben operar de forma similar a las carteras físicas, aceptando cualquier credencial estandarizada. También deben poder ser instaladas en cualquier dispositivo.

Las carteras SSI deben trabajar con un agente digital para establecer conexiones y realizar el intercambio de credenciales. Por último, es importante que estas carteras puedan realizar una copia de seguridad y mover los datos de una cartera digital a otra según sea necesario.

2.1.1.4 Agentes digitales

Las aplicaciones o módulos de software conocidos como agentes digitales permiten el uso de billeteras digitales para obtener y presentar credenciales, gestionar conexiones y comunicarse de forma segura con otros agentes digitales. Los agentes digitales son esenciales para hacer más fluida la comunicación entre los distintos participantes del entorno de la identidad soberana.

2.1.1.5 Identificadores descentralizados (DID)

Necesitamos una forma segura, escalable y sólida para que los titulares de las identidades y sus agentes puedan demostrar la propiedad de sus claves públicas, para poder lograr una mensajería descentralizada entre agentes y carteras digitales en la que sea seguro el intercambio de VC. Al ser la PKI convencional demasiado costosa, pesada y centralizada para satisfacer las necesidades de una infraestructura SSI, surgió como solución un nuevo tipo de identificador, los DID, que debe cumplir con las siguientes propiedades:

- Permanente/Permanet: el identificador tiene que ser capaz de no cambiar nunca.
- Resoluble/Resoluable: El identificador debe ser capaz de recuperar no sólo la clave o claves públicas actuales del propietario de la identidad, sino también las direcciones actuales para llegar al agente o agentes del propietario.
- Criptográficamente verificable/Cryptographically verifiable: El titular de la identidad necesita poder demostrar, mediante criptografía, que controla la clave privada asociada a ese identificador.

- Descentralizado/Descentralized: Este nuevo tipo de identificador debe poder evitar puntos únicos de fallo utilizando redes descentralizadas como blockchains, libros de contabilidad distribuidos, tablas hash distribuidas, sistemas de archivos distribuidos etc.

Para finalizar vamos a ver 5 propiedades que las conexiones DID a DID aportan a las relaciones digitales:

- Permanente: La conexión nunca se interrumpirá a menos que una o ambas partes lo deseen.
- Privada: Todas las comunicaciones a través de la conexión pueden ser automáticamente cifradas y firmadas digitalmente.
- De extremo a extremo: La conexión segura no tiene intermediarios.
- Confiable: La conexión admite el intercambio de VC para establecer la confianza a cualquier nivel de seguridad requerido.
- Extensible: La conexión puede utilizarse para cualquier otra aplicación que necesite comunicaciones digitales seguras, privadas y fiables.

2.1.1.6 Blockchain y otros registros de datos verificables

Una blockchain es una base de datos distribuida con un alto grado de resistencia a la manipulación que puede estar controlada por una o varias entidades. Puede proporcionar una fuente de datos autorizada en la que varios pares pueden confiar sin ninguno tener control absoluto. Es fundamental resaltar que una blockchain debe ser diseñada e implementada con cuidado para resistir ataques. Comparados con otros identificadores electrónicos, las blockchains ofrecen diversas ventajas. En primer lugar, ofrecen una fuente de datos confiable y autorizada que no se basa en una autoridad central de confianza, es decir, los datos almacenados en una blockchain pueden ser verificados y confiados por múltiples partes sin necesidad de intermediarios. Además, ofrecen transparencia y trazabilidad, todas las transacciones quedan registradas y conectadas criptográficamente a las transacciones previas, lo que posibilita el seguimiento del historial de operaciones. La integridad de los datos almacenados en la blockchain se ve reforzada, lo que genera mayor seguridad y confianza. Además, por su naturaleza distribuida y la criptografía usada para

verificar las transacciones, es complicado modificar los datos almacenados sin descubrirse.

2.1.1.7 Marcos de gobernanza

El marco de gobernanza regula el uso de la infraestructura de identidad soberana con reglas y normas empresariales, legales y técnicas. El principal objetivo es establecer políticas y procedimientos para que los emisores puedan emitir credenciales de manera fiable y segura. El marco de gobernanza también define las responsabilidades y obligaciones de las partes involucradas en el ecosistema de confianza digital, estos roles pueden incluir requisitos de seguridad, estándares técnicos, políticas de privacidad y otros aspectos relacionados con la emisión y verificación de credenciales. Estas partes involucradas son emisores de credenciales, verificadores, titulares de las credenciales y autoridades de gobernanza.

Finalmente, este marco es importante porque permite la formación de comunidades de confianza en cualquier tamaño y alcance. Esto quiere decir que puede ajustarse a una comunidad de confianza local, así como a toda una industria.

2.1.2 Trust over IP (ToIP)

ToIP [7] es un modelo arquitectónico de 4 capas para infraestructuras de confianza digital, que responde a la pregunta de ¿Cómo combinar estos siete elementos para formar una imagen general y coherente de la infraestructura SSI? Este proyecto de la Fundación Linux presenta una pila de 4 capas para respaldar ecosistemas de confianza digital interoperables.

[7] https://trustoverip.org/

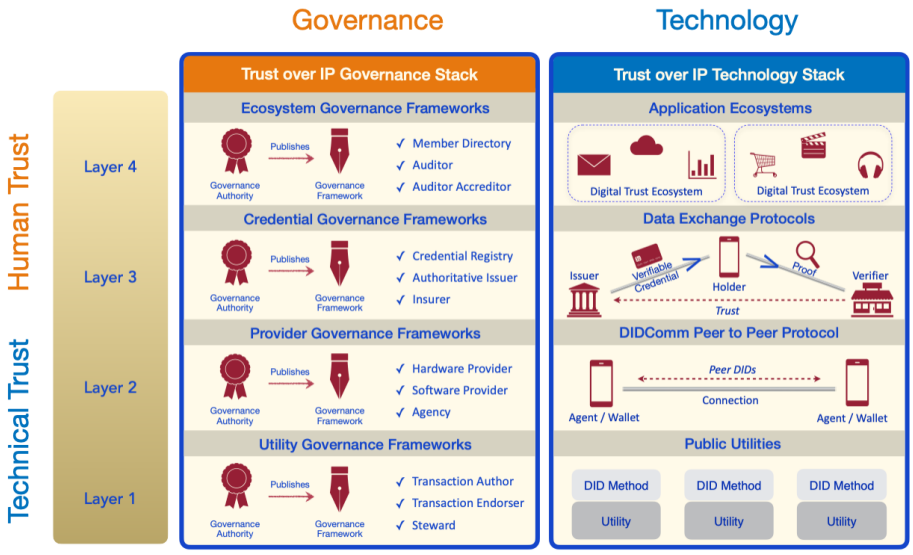


Ilustración 1 El doble "Trust over IP Stack"

Esta pila presenta dos visiones distintas:

- La pila de gobernanza, que trabaja para definir modelos y normas de interoperabilidad para marcos de gobernanza que permitan la confianza empresarial, jurídica y social entre entidades que apliquen la arquitectura de la pila ToIP.
- La pila tecnológica, define las normas técnicas, los conjuntos de pruebas y las normas de certificación de interoperabilidad para la arquitectura de la pila ToIP.

Se pueden observar cuatro capas, las dos capas inferiores se centran en el cumplimiento de los requisitos técnicos de la confianza digital, mientras que las dos capas superiores se centran en el cumplimiento de los requisitos humanos.

En la **capa 1** se definen los marcos de gobernanza para servicios públicos, como blockchain, con el objetivo de asegurar la confianza en las políticas y procedimientos utilizados en la operación de servicios de Identificadores Descentralizados (DID). La gobernanza cambia dependiendo de la arquitectura criptográfica usada, ya sea pública sin permiso como Bitcoin o con permiso como Sovrin o como Alastria.

En la **capa 2** se establecen estructuras de gobierno para carteras/agentes digitales, con el fin de garantizar normas de seguridad, privacidad, protección

de datos e interoperabilidad entre ellos, para así poder almacenar e intercambiar credenciales digitales a través de un protocolo estándar entre iguales como DIDComm.

En la **capa 3** es donde hacemos la transición de la confianza técnica a la confianza humana. En esta capa se definen estructuras de gobierno para las credenciales, usando normas de confianza para que los verificadores puedan tomar decisiones basándose en credenciales comprobables.

La **capa 4** es para las aplicaciones de mercado, necesarias para construir ecosistemas de confianza digital sanos y vibrantes sobre esta nueva infraestructura de confianza digital descentralizada.

2.2 DLT (Distributed Ledger Technology)

Las bases de datos descentralizadas y gestionadas por varias entidades son conocidas como tecnologías de registros distribuidos (DLT)[8]. Esto significa que habrá varias copias idénticas distribuidas entre las entidades y serán actualizadas de forma sincronizada mediante consenso. A diferencia de las bases de datos distribuidas tradicionales, en un DLT no hay una confianza total entre las partes, por lo que se necesita un mecanismo de verificación colectiva antes de compartir registros. Para lograr la autenticidad, integridad y consistencia de los datos almacenados, la tecnología DLT combina redes peer-to-peer, criptografía asimétrica y algoritmos de consenso.

Por lo tanto, de manera más sencilla podríamos decir que un DLT es un sistema que almacena y maneja transacciones y registros de datos sobre una red descentralizada. En lugar de una sola entidad centralizada que controla y administra la base de datos, DLT permite que varias entidades mantengan una copia similar de la base de datos en tiempo real y sincronizada, lo cual mejora la transparencia, seguridad y eficiencia en el manejo de los datos y las transacciones.

[8] https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp

2.2.1 Blockchain

La tecnología blockchain es un tipo de tecnología de registro compartido (DLT) en la cual las transacciones son realizadas directamente entre pares (peer-to-peer) y se realiza mediante bloques, es decir, las transacciones se registran y se agrupan en bloques donde cada bloque nuevo queda ligado al anterior (incluyendo el hash del anterior bloque) para así formar una cadena de bloques.

2.2.1.1 Tipos de blockchain

Existen diversas redes blockchain en función de los requerimientos y casos de uso, en este apartado nos vamos a centrar en los tres tipos principales:

- Blockchain publica: Este tipo de blockchain está abierto a la participación y al acceso de cualquier entidad, ya que no hay sistemas de permisos. A través de esta red una entidad puede realizar transacciones de manera transparente. Un problema de este tipo de redes es el rastreo de la trazabilidad. Dos redes muy conocidas son Bitcoin y Ethereum.
- Blockchain privada: Es una red privada que puede funcionar en entornos donde requieran algunas de las ventajas de la tecnología blockchain y a su vez requieran que el control de los datos sea centralizado, como puede ser en una compañía. Por tanto, es una cadena de bloques con permisos, donde una entidad centralizada controla y administra la cadena. Dicha entidad proporciona permisos a los usuarios para participar en las transacciones y validaciones de los bloques. Un ejemplo puede ser Ripple.
- Blockchain permisionada: Este tipo de red blockchain busca combinar las características de las blockchain públicas como de las privadas. En este tipo de red, los nodos que van a participar en la red son seleccionados (esto correspondería a la parte privada), pero las transacciones que se van a realizar son públicas y visibles para todos (esto correspondería a la parte pública). Un ejemplo puede ser Evernym o Alastria.

Tipo Blockchain	Descripción	Ejemplos
Blockchain no permisionada pública	Abierto a todo el mundo con conexión a Internet para participar en los mecanismos de consenso blockchain, para realizar transacciones y observar el registro completo de transacciones.	Bitcoin Litecoin
Blockchain permisionada pública	Permite a todo el mundo con conexión a Internet ver el registro de transacciones, pero sólo un número restringido de participantes puede contribuir a los mecanismos de consenso.	Ripple Private version of Ethereum
Blockchain permisionada privada	Restringe las transacciones y el acceso para ver el registro de transacciones a los nodos participantes en el sistema. El arquitecto (o propietario) de la cadena de bloques puede determinar quién puede contribuir al sistema de cadena de bloques y qué nodos pueden participar en los mecanismos de consenso.	Rubix Hyperledger
Blockchain no permisionada privada	Restringido en cuanto a quién puede realizar transacciones y ver el registro de transacciones. El mecanismo de consenso está abierto a cualquiera.	Exonum (Partially)

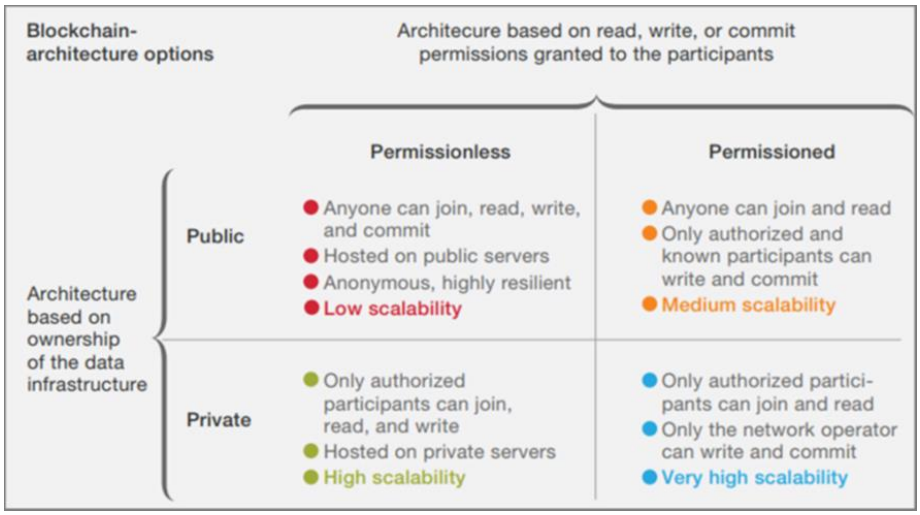


Ilustración 2 [9] Opciones y diferencias de la arquitectura Blockchain

[9] Tabla e ilustración: https://www.itu.int/en/ITU-T/focusgroups/ai4ee/Documents/TS-D.WG2_05-Guidelines%20on%20Energy%20Efficient%20Blockchain%20Systems_Anthopoulos_Nikolau.docx

2.3 ERC 725 y ERC 735

En octubre de 2017, Fabian Vogelsteller, un destacado desarrollador de Ethereum conocido por sus contribuciones como el navegador Mist, Web3.js y el estándar ERC20, presentó la solicitud de comentario 725 de Ethereum (ERC725) en GitHub.

ERC725[10] se configura como un sistema de identidad digital, estableciendo funciones estándar para crear identidades únicas para personas, grupos, objetos y máquinas. Estas identidades pueden contener claves para firmar diversas acciones, tales como transacciones, documentos e inicios de sesión, así como afirmaciones que pueden ser validadas tanto por terceros como por uno mismo (ERC735[11]). Adicionalmente, incorpora una función de proxy que facilita el trabajo directamente en la Blockchain. Esta interfaz estándar permitirá a las aplicaciones descentralizadas (Dapps), contratos inteligentes y terceros verificar la autenticidad de una entidad en solo dos pasos.

Las ventajas de este sistema son claras. Hoy en día, múltiples entidades recopilan información sobre las personas para identificarlas (nombre, apellidos, fecha de nacimiento, usuario y contraseña, entre otros datos). Con un estándar como ERC725, sería posible verificar la identidad mediante una entidad de confianza sin necesidad de almacenar datos reales de los usuarios, reduciendo así el riesgo de pérdidas o filtraciones no autorizadas y asegurando que los datos permanezcan bajo el control de su legítimo propietario.

Por lo tanto, ERC-725 es un estándar que permite publicar y administrar identidades en la cadena de bloques basada en Ethereum. Este estándar describe contratos inteligentes de proxy que pueden ser controlados mediante múltiples claves. Y, ERC-735 permite la emisión de reclamaciones en billeteras o contratos de identidad basados en ERC-725. ClaimHolder hereda de KeyHolder e implementa las funciones definidas en ERC-735. Un aspecto

---

[10] https://ethereum.stackexchange.com/questions/57851/erc725-with-erc735-identity-and-claims

[11] https://www.linkedin.com/pulse/identidad-digital-y-reclamaciones-erc-725erc-735-jose-z%C3%A1rate/

crucial del contrato es que el ID de reclamo se calcula utilizando keccak256 y que cada reclamo se agrega a través de la función addClaim(), sin necesidad de un constructor. Cualquier persona puede implementar este contrato para tener una identidad en la red Ethereum y agregar los contratos ClaimHolder de los emisores cuyas reclamaciones desea aceptar.

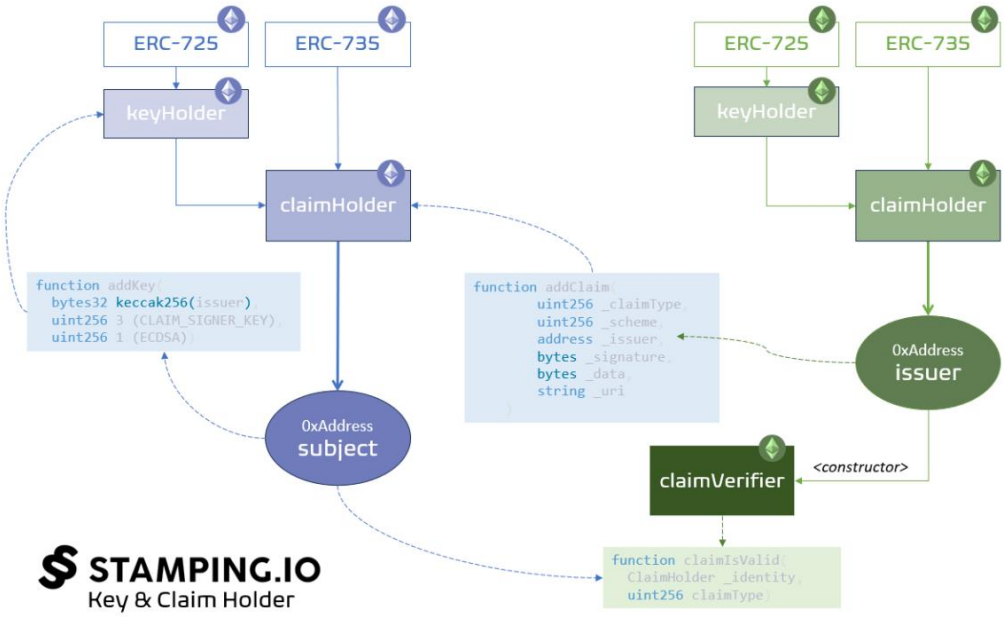


Ilustración 3 Esquema Ethereum, estándar ERC 725 y ERC 735

La relación entre estos dos estándares está en que ERC 735 se encarga de la gestión de las reclamaciones realizadas sobre una identidad ERC 725.

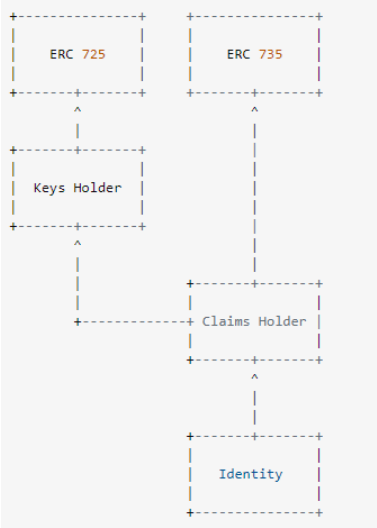


Ilustración 4 ERC 725 y ERC 735

3 Análisis de los principales modelos y marcos de identidad digital internacionales

En esta sección nos vamos a centrar en la búsqueda de los principales modelos y marcos de identidad digital en los distintos continentes.

3.1 América (del Norte)

3.1.1 Estados Unidos

Actualmente, en Estados Unidos la identificación ciudadana se basa principalmente en documentos emitidos por el gobierno, como licencias de conducir, tarjetas de seguro social y pasaportes. Esto representa una gran problemática en muchos aspectos, empezando por el fraude de identidad, ya que son documentos fácilmente falsificables, lo que acaba provocando que numerosos delincuentes acaben cometiendo una gran variedad de delitos como robo de identidad, fraude financiero, lavado de dinero etc. A través del modelo SSI el objetivo es conseguir una reducción del fraude, mejorando así la autenticación y verificación de identidad, previniendo de esta manera el fraude y el robo de identidad.

NIST SP 800-63

El SP 800-63[12] es un documento de pautas y directrices de identidad digital proporcionado por el Instituto de Estándares y Tecnologías (NIST). Este documento describe los marcos de identidad generales, con autenticadores, credenciales y afirmaciones, y un proceso basado en riesgos para seleccionar niveles de garantía. Los requisitos contenidos en este documento proporcionan orientación específica relacionada con el riesgo de la identidad digital mientras se ejecutan todas las fases relevantes del ciclo de vida del RMF (Marco de gestión de riesgos).

En este documento se establecen distintos niveles de garantía. Para los sistemas no federados, las agencias seleccionarán dos componentes:

[12] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

- Nivel de garantía de identidad (IAL), se refiere al proceso de prueba de identidad
- Nivel de garantía del autenticador (AAL), se refiere al proceso de autenticación.

Para los sistemas federados. Se incluye un tercer componente:

- Nivel de garantía de Federación (FAL), se refiere al protocolo de aserción utilizado en un entorno federado para comunicar información de autenticación y atributos (si corresponden) a un RP (partes que confían).

El SP 800-63 está organizado como un conjunto de volúmenes, en los que se utiliza los niveles de garantía mencionados anteriormente. Estos son:

SP 800-63-3

Pautas y directrices de identidad digital: proporciona la metodología de evaluación de riesgos y una visión general de los marcos generales de identidad. Este volumen es una actualización y reestructuración de SP 800-63-2. SP 800-63-3 presenta los componentes individuales de garantía de autenticación digital: AAL, IAL y FAL. Estos componentes se introducen para abordar la creciente demanda de una evaluación independiente de la fortaleza de la autenticación y la confianza en la identidad declarada de un individuo, como en el caso de la autenticación seudónima fuerte.

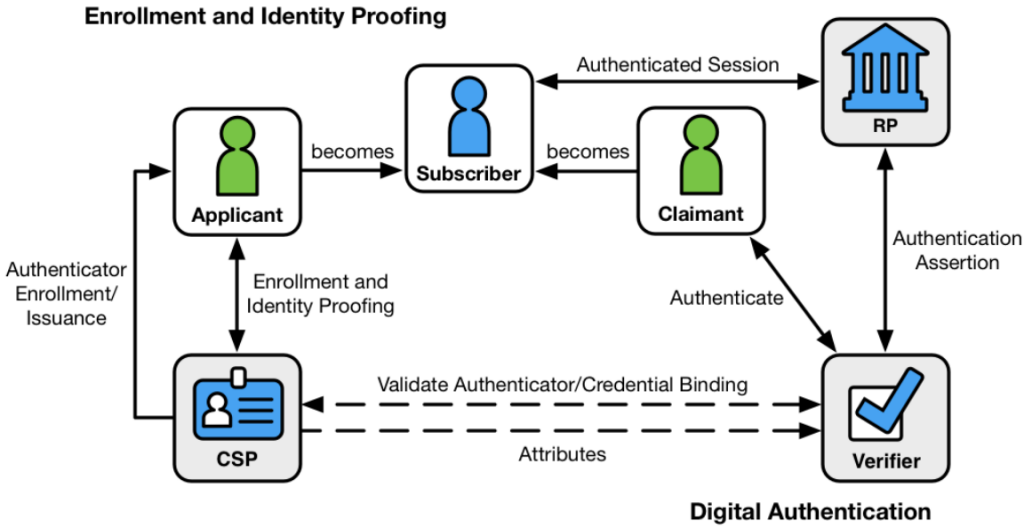


Ilustración 5 Digital Identity Model

SP 800-63A

Inscripción y comprobación de identidad: Trata de cómo los solicitantes pueden demostrar sus identidades y ser registrados como sujetos válidos en un sistema de identidad. Proporciona los requisitos para los procesos que permiten a los solicitantes probar e inscribirse en uno de los tres niveles diferentes de mitigación de riesgos, tanto en escenarios remotos como físicamente presentes.

SP 800-63A establece requisitos para lograr un IAL determinado. Los tres niveles de IAL presentan las opciones para que las agencias puedan seleccionar en base a su perfil de riesgo y al daño potencial causado por un atacante que logre hacer una afirmación falsa exitosa sobre una identidad. Estos tres niveles IAL son:

IAL1: No es necesario vincular al solicitante con una identidad específica de la vida real. Cualquier atributo proporcionado junto con el proceso de autenticación son autoafirmados o debe tratarse como tal.

IAL2: La evidencia respalda que la identidad reclamada existe en el mundo real y verifica que el solicitante está correctamente asociado a esta identidad en el mundo real. En IAL2 es necesario realizar pruebas de identidad presencialmente o a distancia, utilizando como mínimo los procedimientos indicados en SP 800-63A.

IAL3: Es necesaria la presencialidad del solicitante para probar la identidad. Los atributos de identificación deben ser verificados por un representante autorizado del CSP (Proveedor de servicios de credenciales).

SP 800-63B

Autenticación y gestión del ciclo de vida: Aborda cómo una persona puede autenticarse de manera segura en un CSP para acceder a un servicio digital o a varios servicios digitales. Este volumen también describe el proceso de vinculación de un autenticador a una identidad.

Los tres nivelen AAL determinan las opciones que las agencias pueden elegir dependiendo de su nivel de riesgo y del posible daño causado por un atacante que tome el control de un autenticador para acceder a los sistemas. Estos tres niveles AAL son:

AAL1: Ofrece cierta garantía de que el solicitante controla un autenticador registrado a nombre del abonado. AAL1 requiere autenticación de factor único o multifactor utilizando diversas tecnologías de autenticación. Para que sea satisfactoria la autenticación, el solicitante debe demostrar la posesión y el control del autenticador mediante un protocolo de autenticación seguro.

AAL2: Ofrece una gran confianza en que el solicitante tiene bajo control los autenticadores registrados a nombre del abonado. Es necesario demostrar la posesión y el control de dos factores de autenticación distintos mediante uno o varios protocolos de autenticación seguros. AAL2 requiere el uso de técnicas criptográficas aprobadas.

AAL3: Proporciona una confianza muy alta en que el reclamante controla los autenticadores registrados para el abonado. La autenticación en AAL3 se basa en la prueba de la posesión de una clave mediante un protocolo criptográfico. Este es como AAL2, pero requiere además un potente autenticador criptográfico que proporcione resistencia a la suplantación del verificador.

SP 800-63C

Federación y aserciones: Detalla los requisitos para el empleo de arquitecturas de identidad federada y aserciones con el fin de enviar los resultados de las verificaciones de autenticación y la información pertinente a la identidad a una aplicación de la agencia. Además, este volumen ofrece técnicas para mejorar la privacidad al compartir información sobre un sujeto válido y autenticado, además, describe métodos que permiten realizar una autenticación multifactor fuerte (MFA) mientras el sujeto permanece como seudónimo para el servicio digital.

Las tres FAL muestran las opciones que las agencias pueden elegir según su perfil de riesgo y el posible daño causado por un atacante que tome el control de las transacciones federadas. Los tres niveles FAL son:

FAL1: Permite al RP recibir una afirmación de portador de un proveedor de identidad (IdP). El IdP debe firmar la afirmación utilizando criptografía aprobada.

FAL2: Añade el requisito de que la aserción se cifre utilizando criptografía aprobada de forma que el RP sea la única parte que pueda descifrarla.

FAL3: El suscriptor debe presentar una prueba de posesión de una clave criptográfica que se menciona en la aserción, junto con la propia aserción. La aserción es firmada por el IdP y cifrada al RP mediante criptografía aprobada.

3.1.2 Canadá

Marco Fiduciario Pancanadiense (PCTF)

El Pan-Canadian Trust Framework[13] (PCTF) es un marco que abarca numerosos conceptos, definiciones, procedimientos y criterios acordados junto con un enfoque de evaluación. Busca estandarizar la forma en que los gobiernos en Canadá y a nivel internacional crean, emiten y aceptan identidades digitales, tanto dentro de diferentes jurisdicciones como entre distintos sectores. Aunque no es un estándar en sí mismo, el PCTF es un marco que conecta y emplea normas, políticas, directrices y prácticas existentes. Cuando no hay tales normas y políticas, especifica criterios adicionales. Así, su función es complementar las normas y políticas existentes, como las relacionadas con seguridad, privacidad y prestación de servicios.

Este modelo ha sido diseñado para utilizar marcos internacionales de identidad digital como:

- Los Servicios de Identificación Electrónica, Autenticación y Confianza (eIDAS).
- El Grupo de Acción Financiera Internacional (GAFI).
- La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).

Por último, cabe destacar que PCTF no es un marco de gobernanza formal, sino que es una herramienta para ayudar a evaluar un programa o servicio de identidad digital.

[13] https://diacc.ca/trust-framework/

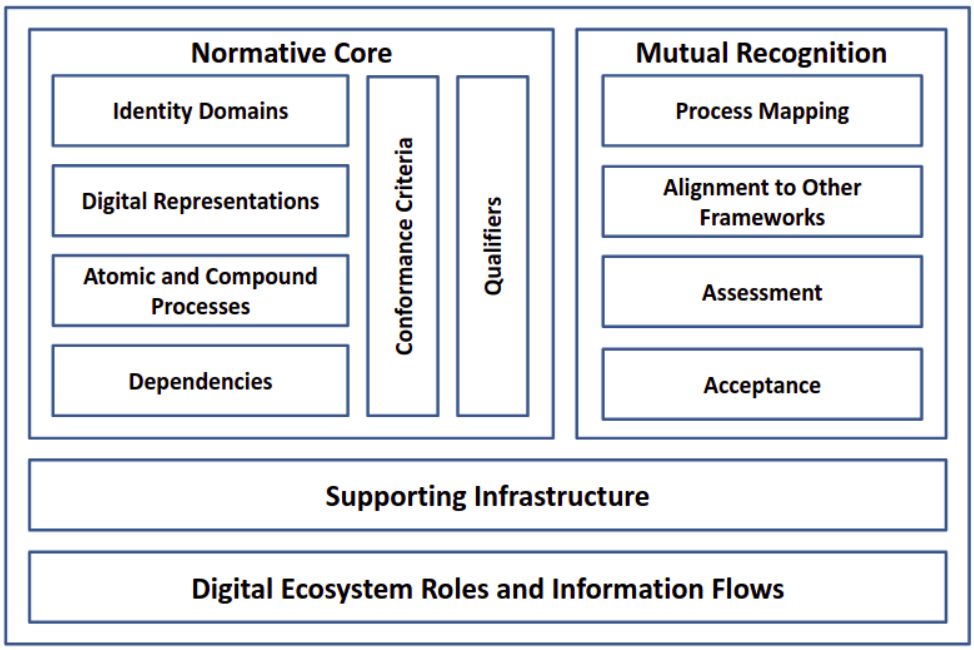


Ilustración 6 El modelo Pan-Canadian Trust Framework

Como vemos en la ilustración de arriba, encontramos un diagrama con los componentes principales del modelo PCTF.

Núcleo normativo/Normative core: este componente encapsula los conceptos clave de PCTF.

Representaciones Digitales: En este apartado se describen las entidades, sus relaciones correspondientes y los atributos que las distinguen en el contexto del PCTF. Los elementos o sujetos que participan en el entorno digital pueden ser individuos, organizacionales o dispositivos, estos se conocen como entidades. Estas entidades se relacionan y tienen vínculos a través de las relaciones. En cuanto a los atributos, estos ayudan a definir tanto las entidades como las relaciones al identificarlas por sus características o propiedades únicas

Tipos de Identidad: Se consideran varios tipos de identidad en este contexto. Este grupo incluye identidades concretas vinculadas a personas reales, así como identidades virtuales o digitales que se expresan a través de cuentas de usuario o perfiles en línea. Entender esta variedad de identidades es crucial para la creación de sistemas digitales seguros y fiables.

Procesos Atómicos y Compuestos: Dentro del marco del PCTF, se detallan los procedimientos empleados para administrar las identidades en esta área. Los procesos atómicos son acciones individuales que se realizan para administrar una identidad, como la creación de una cuenta o la verificación de información personal. Se conocen como procesos compuestos a las combinaciones de procesos atómicos ejecutados en secuencia para lograr un objetivo específico.

Dependencias: En este ámbito se aborda el análisis de las interrelaciones entre los distintos componentes del mismo. Este enfoque se centra en identificar las conexiones y requisitos mutuos entre los elementos del marco. La correcta operación de ciertos aspectos o elementos del PCTF se encuentra condicionada por el funcionamiento adecuado de otros. Esta interdependencia entre los diversos componentes del marco garantiza la coherencia en su implementación y facilita la interoperabilidad entre ellos.

Criterios de Conformidad: En esta sección, se establecen los criterios para que los actores del ecosistema digital garanticen la confianza y la interoperabilidad. Deben seguirse estos criterios como requisitos y directrices para cumplir con los estándares del PCTF, ya que para garantizar la seguridad y la confianza en los servicios digitales y en el intercambio de información es fundamental cumplir con estos criterios.

Calificadores: Se usan para brindar mayor detalle y especificidad a los criterios de conformidad dentro del PCTF. Dependiendo de los casos en los que sea aplicable, un criterio de conformidad puede tener un solo calificador o varios. Estos indicadores ayudan a especificar y asignar los estándares de cumplimiento con relación a otros marcos de confianza, lo que simplifica la interoperabilidad y la comparación entre diferentes normas.

Reconocimiento mutuo/Mutual recognition: describe la metodología actual utilizada para evaluar y certificar a los agentes del ecosistema digital. El reconocimiento mutuo es un acuerdo por el que dos o más partes acuerdan reconocer los resultados de una evaluación de conformidad. Dependiendo del contexto, el reconocimiento mutuo puede formalizarse mediante la emisión de una carta de aceptación o formar parte de un acuerdo más amplio. Antes de iniciar el proceso de reconocimiento mutuo del PCTF, se recomienda emprender

un proceso de planificación y compromiso con los principales participantes para desarrollar un acuerdo de trabajo formalizado.

Mapeo de Procesos: El proceso de mapeo consiste en identificar y documentar las actividades y los flujos de trabajo relacionados con el reconocimiento mutuo. Se puede comprender cómo se lleva a cabo el proceso y su relación con otros aspectos del marco utilizando este mapeo.

Alineación con Otros Marcos: En esta sección se refleja la importancia de alinear el proceso de reconocimiento mutuo con otros marcos y estándares internacionales. Se buscan alinear algunos marcos como el Marco de elDAS, el Grupo de Acción Financiera Internacional (GAFI) y la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).

Evaluación: En esta sección se aborda el proceso de evaluación que se lleva a cabo en el reconocimiento mutuo. Se enumeran los criterios y requisitos que deben cumplirse para reconocer los resultados de una evaluación de conformidad. Esto puede implicar la revisión de documentación, pruebas y verificación del cumplimiento de estándares específicos durante la evaluación.

Aceptación: El proceso de aceptación sigue al reconocimiento mutuo. Las partes involucradas acuerdan reconocer los resultados de la evaluación de conformidad y formalizar este reconocimiento a través de un documento, como una carta de aceptación. Es crucial para construir la confianza y la interoperabilidad entre las partes.

Infraestructura de apoyo/Suporting infrastructure: describe el conjunto de políticas, reglas y normas operativas y técnicas que sirven como principales habilitadores del ecosistema digital. Las distintas normativas de la infraestructura de apoyo quedan excluidas del ámbito del PCTF. El PCTF no establece recomendaciones sobre cómo debe ser la composición de la infraestructura de apoyo.

Algunos elementos que constituirían la infraestructura de soporte son: prestación de servicios digitales, métodos, acuerdos de nivel de servicio, necesidades y experiencia del usuario, mecanismos de transmisión, perfiles de

implementación, privacidad y seguridad, interoperabilidad, evaluaciones de impacto en la privacidad, etc.

Métodos: Los métodos regulan la interacción directa o indirecta entre los agentes del ecosistema digital. Los métodos abarcan elementos como modelos y esquemas de datos, protocolos de comunicación, mecanismos de transmisión, algoritmos criptográficos, bases de datos, libros de contabilidad distribuidos, registros de datos verificables y esquemas similares. Los métodos también pueden incluir sistemas aislados o con conexión interrumpida. El PCTF no recomienda un método sobre otro.

Mecanismos de transmisión: Los métodos mediante los que la salida de un proceso atómico se vuelve disponible para usarse como entrada por otro proceso atómico se conocen como mecanismos de transmisión. Los mecanismos de transmisión se ubican entre las partes que generan y utilizan los estados de salida de los procesos atómicos.

Funciones y flujos de información del ecosistema digital/ Digital Ecosystem Roles and Information Flows: define las funciones y los flujos de información dentro del ecosistema digital. En esta sección se define el modelo de roles del ecosistema digital definido en el PCTF. Estos son:

- Sujeto: Es una entidad sobre la cual se afirman reclamaciones por parte de un emisor. El sujeto puede ser una persona, una organización u otra entidad.
- Emisor: Es una entidad que afirma una o más reclamaciones sobre uno o más sujetos. El emisor crea una credencial a partir de estas reclamaciones y asigna la credencial a un titular.
- Titular: Es una entidad que posee una credencial emitida por un emisor. El titular puede ser un sujeto o una entidad que actúa en nombre de un sujeto.
- Verificador: Es una entidad que verifica la validez y la autenticidad de una credencial presentada por un titular. El verificador puede ser una organización o una entidad que requiere la verificación de la identidad o las cualificaciones de un sujeto.

Por último, el modelo consta de cinco flujos de información:

- Reclamación: declaración sobre un sujeto o sobre una asociación existente entre dos o más sujetos. Las reclamaciones son presentadas por los emisores.
- Credencial: Afirmación de identidad, cualificación, competencia, autoridad, derechos etc. Una credencial contiene un conjunto de una o más afirmaciones afirmadas sobre uno o más sujetos.
- Presentación: Información derivada de una o más credenciales. La fuente "credenciales" pueden haber sido emitidas por diferentes emisores.
- Registro de Credenciales: Declaración efectuada por el emisor de que éste emite un tipo de credencial. La declaración puede incluir una definición del formato de la credencial.
- Confirmación de presentación: Determinación por parte del verificador de la corrección de la presentación.

3.2 América (del Sur)

3.2.1 Brasil

En Brasil, las autoridades gubernamentales están realizando pruebas de concepto para explorar el potencial de las tecnologías de registros distribuidos (DLT). En los últimos años, se han logrado avances significativos en la identificación digital en el país. Fue creada una infraestructura de clave pública llamada ICP-Brasil para permitir el uso de firmas digitales y verificar la integridad de documentos. En 1997, se comenzaron a realizar esfuerzos para poner en marcha un servicio nacional de identidad digital y desde entonces se ha notado un progreso significativo. En el año 2008, se comenzó a registrar a los ciudadanos en el Tribunal Superior Electoral mediante datos biométricos. Más tarde, en 2017, se aprobó por ley federal la creación del Documento Nacional de Identidad (DNI), lo que establece un identificador civil nacional conocido como Identificação Civil Nacional (ICN).

CPQD

Desde 2016, el CPQD [14] (Centro de Pesquisa e Desenvolvimento em Telecomunicações) ha estado trabajando en Blockchain, desarrollando formación tecnológica, estableciendo alianzas, creando soluciones y difundiendo conocimiento para contribuir a la evolución de esta tecnología en Brasil, tanto en el sector privado como en el gobierno. CPQD es un referente nacional e internacional en soluciones para Blockchain, proporcionando implementación de redes, desarrollo de soluciones y componentes, así como herramientas de gobierno del sistema para satisfacer las necesidades de las empresas y socios.

El **CPQC iD** es una solución de identidad digital descentralizada, que no es lo mismo que el concepto de SSI, ya que es posible ser descentralizado sin ser autogestionado. Posee un conjunto de APIs que permiten definir, emitir y autenticar credenciales almacenadas en una billetera digital. Esto aporta confianza y valor a los procesos de incorporación, autenticación, autorización y firma digital, haciendo de esta manera seguras las conexiones a internet.

En esta solución, el intercambio de información se realiza de acuerdo con la LGPD (la ley general de protección de datos brasileña) y el RGPD. Las credenciales de identidad digital se almacenan en una aplicación de billetera digital en el teléfono, sin almacenar datos en la nube, de esta manera CPQD iD reduce drásticamente el riesgo de fuga de información y le da al usuario el control de sus datos. Su funcionamiento se da a través de la emisión de una credencial verificable que se personaliza de acuerdo con la necesidad y nivel de seguridad que se requiere.

[14] https://www.cpqd.com.br/es/

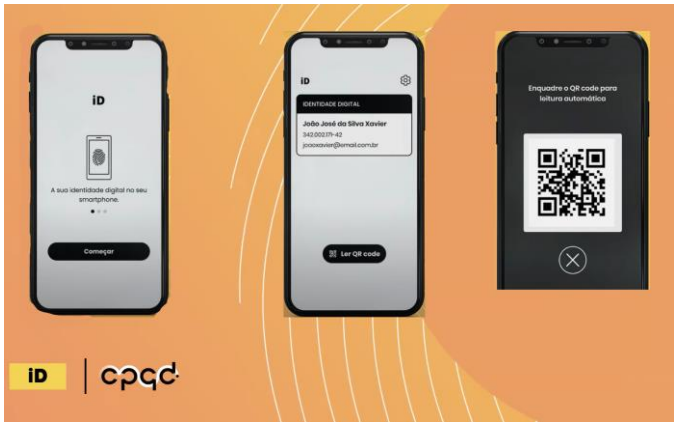


Ilustración 7 CPQDiD caso de uso

En cuanto a la actualidad, siguiendo el decreto del 25 de septiembre, todo el país brasileño deberá poder emitir documentos de identidad digital sustentados en blockchain. El Documento Nacional de Identidad (CIN), es utilizado ya por tres millones de brasileños, el documento fue diseñado por el Ministerio de Gestión e Innovación en Servicios Públicos para reemplazar el antiguo documento de identidad, utiliza el CPF (Cadastro de Pessoas Físicas, el documento de identificación fiscal brasileño) como número de identificación único, y utiliza distintas tecnologías Sepro para aumentar y garantizar la seguridad de la información y sincronizar los datos.

En definitiva, es un revolucionario proyecto que mejorará los servicios públicos y privados, permitiendo a los ciudadanos acceder a servicios como la salud, la seguridad social, la educación o el transporte, a través de esta identidad digital. Además, en Brasil, con la crisis del COVID-19, se estimó que 30 millones de personas quedaron fuera de los registros gubernamentales. La identidad digital sería el medio para acercar la población invisible a la realidad social y democrática de las ciudades inteligentes, y una forma de hacer efectivos los derechos humanos fundamentales, como el derecho a la alimentación, la vivienda, la salud, la educación, el trabajo, la seguridad social, la inclusión social y digital, entre otros, para el desarrollo humano.

3.2.2 México

En México, la base legal de la identidad se encuentra en la Constitución Política, que garantiza el derecho a tener una identidad y a ser registrado al nacer. A través de la Clave Única de Registro de Población (CURP) y la Cédula de

Identidad Ciudadana, se define la identidad en base al concepto desarrollado por la Ley General de Población. La CURP y la Cédula de Identidad Ciudadana son dos documentos oficiales que se otorgan a cada persona al nacer, contiene información única e irrepetible, como el nombre, la fotografía y la firma del titular. Según la Ley Federal de Protección de Datos Personales en Posesión de Particulares, las personas físicas son propietarias de sus datos personales, esto implica que tienen el derecho de acceder, corregir, cancelar y oponerse al procesamiento de sus datos. Las entidades que manejan información personal solo pueden hacerlo dentro de los límites legales y deben respetar los derechos de las personas titulares.

México, a pesar de ser unos de los países más importante de América del sur, la comunidad SSI se encuentra muy limitada respecto a otros países latinoamericanos. A pesar de ser la segunda mayor economía de América Latina, se encuentra frente a grandes problemas para conseguir la inclusión financiera. Alrededor de un 37% de los adultos mexicanos carecen de acceso a servicios financieros formales. Las economías informales florecen por la falta de identificación formal y por la falta de confianza en instituciones financieras existentes, las poblaciones vulnerables, las comunidades rurales, las mujeres y las personas con ingresos más bajos se ven muy afectados por el acceso financiero limitado.

A través de SSI, incorporándolo en el entorno financiero de México, podríamos transformar la inclusión financiera de manera significativa. Al eliminar los obstáculos asociados con la identidad, SSI permitiría a los individuos acceder a servicios financieros convencionales, fortaleciendo la confianza y la seguridad en las transacciones. Además, fomentaría la educación financiera y respaldaría el desarrollo de los sectores de microfinanzas y pequeñas y medianas empresas (PYME). La adopción de soluciones de SSI en México ayudaría a reducir la brecha de inclusión financiera, capacitando a las personas y estimulando el crecimiento económico, al tiempo que contribuiría a disminuir las diferencias existentes en el país.

3.2.3 Colombia

En Colombia, no existe una definición legal de "identidad", pero la Constitución y el Decreto 1260/1970 se centran en el estado civil como elemento central. Las personas son las dueñas de sus datos personales y la cédula de ciudadanía es el único documento valido para actos oficiales. No hay una regulación específica para la identificación en el ámbito comercial, ni para las entidades que ofrecen este servicio, aunque las entidades de certificación realizan actividades de identificación relacionadas con la firma digital. Los mensajes de datos tienen la misma validez que la forma escrita si cumplen con la Ley de Firma Digital. Respecto a la identidad digital. Actualmente, Colombia cuenta con un marco legal para la identidad digital, la Ley 1286 de 2008, el Decreto 1078 de 2015 y el Decreto 767 de 16 de mayo de 2022. Estas normas establecen los principios y pautas para la gestión de la identidad digital. Respecto a la implementación de la identidad digital, Colombia ha conseguido un gran avance, se han expedido más de 7 millones de cédulas digitales y se han desarrollado distintas aplicaciones que permiten a los ciudadanos acceder a través de su identidad digital. La Registraduría Nacional del Estado Civil es la entidad responsable de la expedición de la cédula digital, pero hay otras entidades que tienen gran influencia en la gestión de identidad digital, estas son el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Superintendencia Financiera de Colombia (SFC).

El plan nacional de identidad digital es fortalecer la seguridad y confianza en las transacciones digitales, facilitar el acceso a servicios en línea e impulsar la economía digital. Todo esto se pretende conseguir a través de la cédula digital, desarrollando un ecosistema de identidad digital interoperable y fortaleciendo la seguridad y privacidad de la información.

La **cédula digital**[15] es un proyecto que se gestó en el año 2018, esta cédula es la forma electrónica del documento de identidad de los colombianos. El proyecto surgió para fortalecer la identificación de los ciudadanos colombianos. Esta ofrece beneficios como: mayor seguridad frente al robo y falsificación de

[15] https://wapp.registraduria.gov.co/identificacion/cedula-digital/

identidad, portabilidad ya que puedes acceder a ella a través de la aplicación de teléfono móvil, facilidad de uso etc. Para poder conseguir la cédula digital debes cumplir con cuatro requisitos: ser mayor de edad, ser colombiano, no tener una cédula física vigente y estar inscrito en el Registro Civil.

Ilustración 8 Cédula Digital Colombia

Existe un proyecto innovador que fue elegido entre más de 100 emprendimientos, por Self-Sovereign Identity Incubator (SSII) para asistir a su programa intensivo en soberanía digital, este es **Xertify**[16]. Es un proyecto que automatiza la creación de títulos, diplomas, certificados, notificaciones y otros documentos académicos utilizando tecnología Blockchain. Xertify cuenta con una cartera digital para los destinatarios de los certificados, garantizando la privacidad.

Funcionamiento de Xertify para el emisor:

- Carga de la plantilla y preservación de la identidad corporativa: El emisor comienza cargando la plantilla del documento que desea que sea firmado electrónicamente por varios actores. El equipo de expertos de Xertify se encarga de preservar la identidad corporativa.
- Carga de los datos de los receptores y configuración de las firmas: Luego, el emisor carga los nombres y correos electrónicos de los destinatarios

[16] https://xertify.co/

que deben firmar el documento. En este paso, se define el orden en que se realizarán las firmas y su ubicación dentro del documento.

- Programación del envío de los documentos: Finalmente, el emisor programa el envío de los documentos a los actores seleccionados.

Funcionamiento de Xertify para el receptor:

- Recepción del correo: El receptor recibe un correo electrónico con la identidad corporativa del emisor que solicita su firma en uno o más documentos. Para proceder, el receptor debe verificar su identidad.
- Verificación de la identidad: El receptor realiza una verificación de identidad para verificar y validar que él es el representante de ese correo electrónico.
- Firma electrónica del documento: El receptor firma el documento electrónicamente a través de un texto o a través del dibujo digital de su firma.

Finalmente, todas las partes reciben un reporte de la emisión de los documentos firmados. Los receptores reciben en su Xertify Wallet un documento que cumple con los estándares de seguridad blockchain y firma electrónica, los cuales cuentan con validez jurídica.

3.2.4 Argentina

Aunque Argentina carece de una definición legal precisa de "identidad", la normativa actual se enfoca en la reidentificación de las víctimas de la dictadura y en aspectos específicos como el DNI. La ley de Protección de Datos Personales considera que todos los datos personales forman parte de la identidad de un individuo, siendo, por tanto, este el titular de estos. La acreditación de la identidad varía según el contexto, aunque el DNI es obligatorio en ciertos trámites con entidades reguladas. En cuanto a las entidades que brindan servicios de identificación, el Decreto 182/2019 establece que los prestadores de servicios de confianza pueden hacerlo, aunque la regulación aún no está completa. Los documentos digitales son legalmente válidos y tienen la misma validez que los documentos físicos, especialmente en el caso de los instrumentos públicos digitales, que son equivalentes a sus contrapartes físicas. La validez de

los instrumentos privados depende de la firma electrónica o digital y se evalúa según el Código Civil y Comercial de la Nación y la Ley de Firma Digital.

Ahora nos vamos a enfocar en un proyecto que tuvo un gran impacto, el proyecto **DIDI**[17]. En 2018 el laboratorio de innovación del Grupo Banco Interamericano de Desarrollo (BID Lab) y ONG Bitcoin Argentina crearon el Proyecto DIDI, el cual está formalmente denominado como "Inclusión cívica social y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de Blockchain". El objetivo de este proyecto de identidad autogestionada fue investigar, implementar y evaluar los alcances de este modelo de identidad aplicado a la inclusión social, cívica y económica de ciudadanos de barrios vulnerables en Argentina. Se desarrolló una aplicación móvil (denominada ai·di), esta funciona como una cartera digital que permite a los usuarios almacenar credenciales vinculados a aspectos sociales, cívicos y económicos.

Desde 2018 el proyecto viene trabajando en la implementación de soluciones digitales a través de un modelo de Identidad autogestionada (SSI) para facilitar los procesos de inclusión social y financiera. Estas soluciones se vienen implementando en asentamientos informales o barrios populares en Buenos Aires (Barrio Padre Mugica, Villa 31 y 31 Bis) y algunas zonas rurales de Santiago del Estero. En 2019, se comenzó a integrar con el Programa Semillas, con trabajo territorial en el Barrio Padre Mugica. El Programa Semillas funciona dentro de la Asociación Civil Ecomanía Conciencia Ambiental desde el año 2016, su objetivo es promover una economía participativa, sustentable y justa. El proyecto DIDI comenzó su trabajo planificando e implementando el modelo SSI en el caso de uso inicial de Semillas. Se acordó colaboración y se asignaron responsabilidades a cada socio del proyecto, cubriendo aspectos tecnológicos, contribuciones de las entidades, interacción con la población beneficiaria, así como la asignación de tiempos y recursos. El proyecto se presentó al equipo de asesoras y a la población beneficiaria de los microcréditos, con el objetivo de establecer una conexión directa entre Semillas y el equipo de asesoría de DIDI.

[17] https://didi.org.ar/

Siguiendo con el objetivo de implementar el modelo de SSI, DIDI desarrolló la aplicación móvil ai·di. En los orígenes se contempló la construcción de una billetera con dinero digital que pudiera captar información, pero debido a una serie de limitaciones de tipo legal se decidió que la aplicación con herramientas basadas en Blockchain se nutra de credenciales emitidas por terceros o a partir de información generada por el comportamiento de los usuarios, incluyendo información y certificados emitidos por entidades públicas y privadas, emitidos por individuos, información patrimonial y transaccional. Durante 2020 se finalizaron los desarrollos individuales y se inició un proceso para su integración, además se habilito un mayor aprovechamiento del potencial de la herramienta en base a las necesidades de la población. Por otro lado, se avanzó en la construcción del módulo multi-blockchain para permitir que los desarrollos trabajen sobre al menos tres redes EVM (Máquina Virtual de Ethereum) compatibles (RSK, Ethereum y LACChain), y se llevó a cabo una auditoría de seguridad de los sistemas identificando posibles vulnerabilidades.

Ilustración 9 Modelo básico de los primeros casos de uso de la app ai·di

Respecto al proceso de concientización y sensibilización, fue crucial para una implementación efectiva del modelo basado en SSI de DIDI, se enfocó en capacitar a las organizaciones seleccionadas para que pudieran utilizar de manera autónoma las tecnologías ai·di y su aplicación. Se comenzó por desafiar la idea de que el uso de las tecnologías digitales es intuitivo, reconociendo que la alfabetización digital requiere un análisis detallado de la organización y de sus usuarios finales. Se diseñó y ejecutó un programa de formación que involucró a actores clave de las organizaciones, utilizando diversas estrategias según los perfiles de los usuarios. En algunas organizaciones, la incorporación de estas tecnologías implicó cambios significativos en los procesos y roles, por

lo que fue importante gestionar expectativas y necesidades para evitar tensiones y demoras. En el caso del Programa Semillas, se inició la capacitación de manera virtual, pero se adaptó a través de un soporte sincrónico por Whatsapp y encuentros presenciales para garantizar una mejor adopción de la aplicación por parte del equipo y los destinatarios finales.

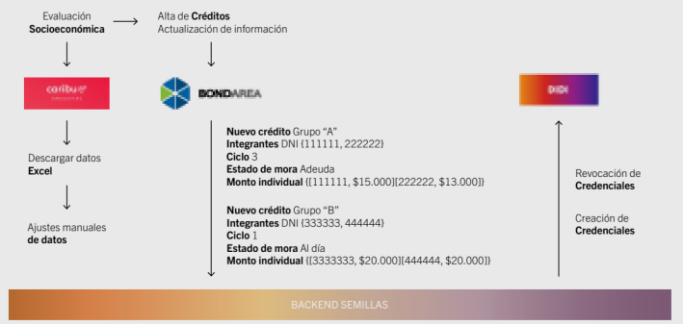


Ilustración 10 Proceso emisión de credenciales programa Semillas

Normas de identidad consideradas bajo el modelo de ai·di:

- La validación de la identidad de las personas se realiza a través del Sistema de Identidad Digital (SID), implementado por el gobierno de Argentina, a través del Ministerio del Interior y la Secretaría de Innovación Pública. Lo que otorga seguridad jurídica y reduce significativamente la posibilidad de fraudes y robos de identidad.
- El SID permite la validación de la identidad a distancia y en tiempo real a partir de la autenticación biométrica con reconocimiento facial, comparando la captura de una fotografía desde un dispositivo móvil con la fotografía del DNI existente en las bases de datos del Registro Nacional de las Personas (RENAPER).
- La aplicación ai·di cuenta con un proceso alternativo de validación de identidad, en el que las personas pueden adjuntar su DNI.
- Al garantizar la autenticación de las personas e interoperar con los servicios del Estado, las personas y los usuarios emisores y verificadores de credencial de identidad tienen plena certeza jurídica de que la persona es quien dice ser, generando un entorno de confianza y reduciendo los riesgos de fraude o robo de identidad.

- Lo anterior, va acorde con el modelo internacional de Reglamento EIDAS de la UE, y la Ley modelo sobre la utilización y el reconocimiento transfronterizo de la gestión de la identidad y los servicios de confianza de la CNUDMI.
- Para la generación del DID se observa el estándar W3C sobre identificadores descentralizados.

3.2.5 Comparativas de los países de Latino América

Las siguientes tablas se han extraído de la investigación llevada a cabo por Andrés Chomczyk, entre los años 2019 y 2020. Este informe se denomina "Regulación de blockchain e identidad digital en América Latina | El futuro de la identidad digital".

	Habeas Data	Acceso	Rectificación	Cancelación	Oposición	Olvido	Portabilidad	Bloqueo	Automatizadas
Argentina	×	×	×	×	×				
Bolivia	×	×*	×*	×*	×*	×*			
Brasil	×	×	×	×	×		×		
Chile	×	×	×	×	×			×	
Colombia	×	×	×	×	×				
Costa Rica	×	×	×	×	×				
Cuba		×**	×**	×**	×**				
Ecuador	×								
Méxíco	×	×	×	×	×				
Panamá	×	×	×	×	×		×		×
Paraguay	×	×							
Perú	×	×	×	×	×				×
República Dominicana	×	×	×	×	×			×	
Uruguay	×	×	×	×	×				×

Ilustración 11 Derechos sobre los datos personales reconocidos en los países de América Latina

Tabla 1: se detallan los derechos que cada jurisdicción reconoce a los titulares de los datos.

Referencias: ** Si bien la Constitución Nacional reconoce ciertos derechos, los mismos no son de aplicación directa y están supeditados al dictado de una ley formal.

País	¿Hay un concepto legal de identidad?	¿Quién es el dueño** de los datos personales?	¿Hay una forma única para acreditar la identidad?	¿Los datos personales pueden ser transferidos al exterior?	¿Tiene validez un documento digital?
Argentina	No	El individuo	No*	No*	Sí
Bolivia	No	El individuo	No	Sí	Sí
Brasil	No	El individuo	No*	No*	Sí
Chile	No	El individuo	No*	No*	Sí
Colombia	No	El individuo	Sí*	No*	Sí
Costa Rica	No	El individuo	Sí*	Sí*	Sí
Cuba	No	El individuo	Sí	Sí*	Sí*
Ecuador	Sí	El individuo	Sí*	No*	Sí
México	No	El individuo	No	No*	Sí
Panamá	No	El individuo	Sí	No*	Sí
Paraguay	No	El individuo	No	Sí	Sí
Perú	Sí	El individuo	Sí*	No*	Sí
República Dominicana	No	El individuo	No	No*	Sí
Uruguay	No	El individuo	No*	No*	Sí

Ilustración 12 Marco normativo para la implementación de un sistema privado de SSI

Tabla 2: resume brevemente las principales características del marco normativo de cada país.

Referencias: * La respuesta proporcionada en este punto no es absoluta y es necesario leer el análisis realizado en el punto 4 de la investigación para tener un conocimiento pleno de la situación.

Marco normativo aplicable a blockchain en países de América Latina

País	¿Hay regulación sobre blockchain?	¿Es válido un acto en formato digital?	¿Hay legislación sobre firma digital?	¿Hay regulación sobre contratos inteligentes?	¿Un contrato inteligente es un contrato?*
Argentina	Sí*	Sí	Sí	Sí*	Sí
Bolivia	Sí*	Sí	Sí	No	Sí
Brasil	No*	Sí	Sí	No	Sí
Chile	No	Sí	Sí	No	Sí
Colombia	No	Sí	Sí	No	Sí
Costa Rica	No	Sí	Sí	No	Sí
Cuba	No	Sí *	Sí*	No	Sí
Ecuador	No	Sí	Sí	No	Sí
México	No	Sí	Sí	No	Sí
Panamá	No	Sí	Sí	No	Sí
Paraguay	No	Sí	Sí	No	Sí
Perú	No	Sí	Sí	No	Sí
República Dominicana	No	Sí	Sí	No	Sí
Uruguay	No	Sí	Sí	No	Sí

Ilustración 13 Marco normativo aplicable a blockchain en países de América Latina

Tabla 3: resume las características del marco normativo para blockchain de cada país.

Referencias: * La respuesta proporcionada en este punto no es absoluta y es necesario leer el análisis realizado en el punto 5 de la investigación para tener un conocimiento pleno de la situación.

3.3 Asia

3.3.1 India

India, bajo el liderazgo del primer ministro Narendra Modi, busca convertirse en un líder global en el ámbito educativo y tecnológico. En la última década, India ha desarrollado una serie de plataformas digitales orientadas a los ciudadanos que han generado un gran cambio en sus vidas. A partir de 2009, el gobierno de India comenzó a desarrollar una infraestructura pública digital, inicialmente conocida como "India Stack", esta, en su página oficial se define como "El nombre con el que se conoce a un conjunto de APIs abiertas y bienes públicos digitales cuyo objetivo es desbloquear las primitivas económicas de la identidad, los datos y los pagos a escala de la población". Mas tarde se renombró como "Infraestructura Pública Digital" (DPI).

Esta infraestructura está compuesta por tres elementos: identidad, pagos y gestión de datos. En cuanto a la identidad, en 2010 se puso en marcha un sistema de identidad digital biométrica, denominado Aadhaar. El sistema asigna a todos los residentes, tanto nacionales como extranjeros en India, un número único de 12 dígitos basado en datos biométricos. Este número es emitido por la Autoridad Única de Identificación de India (AUII) es obligatorio para todos. Se puede utilizar para acceder a servicios bancarios, gubernamentales y para el pago de impuestos. Actualmente lo poseen alrededor de 1400 millones de personas. En cuanto a los pagos, más tarde llegó un nuevo sistema, la Interfaz de Pagos Unificados (UPI), este sistema representó el 73% de los pagos minoristas sin efectivo en el país hasta marzo de 2023. Por último, respecto a la gestión de datos, en 2015 fue lanzado por primera vez la iniciativa del Ministerio de Electrónica y Tecnología de la Información (MeitY), DigiLocker[18]. Esta plataforma permite almacenar documentos fiscales, licencias de conducir, certificados académicos o certificados de vacunación, y acceder a ellos desde cualquier dispositivo con conexión a internet. Además, DigiLocker se integra con diferentes departamentos gubernamentales para ofrecer acceso a documentos digitales emitidos por ellos, simplificando la gestión de trámites y

[18] https://www.digilocker.gov.in/

eliminando la necesidad de llevar consigo copias físicas. Por último, los usuarios necesitan tener un número de Aadhaar para usar DigiLocker.

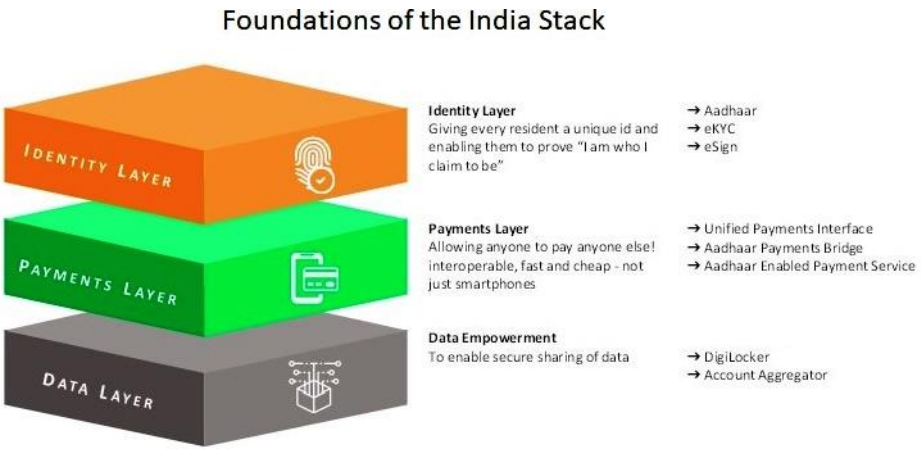


Ilustración 14 Principios de la India Stack

Recientemente en India se aprobó el Digital Personal Data Protection Bill (DPDP), en 2023, esta es una iniciativa del gobierno que busca regular el procesamiento de datos personales digitales en el país. El objetivo principal es proteger la privacidad de los datos y garantizar el uso responsable de los datos por parte de las organizaciones. En este proyecto, el uso de la identidad descentralizada basada el blockchain (el uso del modelo SSI), puede ayudar a abordar distintos aspectos claves del proyecto DPDP, como la identidad autogestionada, el control de acceso detallado, el cifrado irreversible o hashing, las pruebas de conocimiento cero, mayor privacidad y control de los datos, la gestión del consentimiento, seguridad y registros inmutables, auditoría y rendición de cuentas y menor dependencia de las autoridades centrales.

A continuación, vamos a hablar del proyecto **IOMe**[19] de MOI Technology. MOI es un protocolo de blockchain de propósito general centrado en los participantes y construido para el mundo de la interacción digital. MOI es una red de Capa 1 escalable y segura, que permite a cualquiera desplegar activos y aplicaciones, atendiendo a las necesidades específicas y dinámicas de los usuarios. IOMe es

[19] https://iome.ai/

una plataforma de identidad digital descentralizada basada en el protocolo Web3 de MOI. El objetivo es proporcionar a los usuarios el control total de sus datos y a su vez facilitarles una interacción segura con el mundo digital. La base de IOMe reside en la aplicación de Identificadores Descentralizados (DIDs) en una blockchain y en Credenciales Verificables (VC's) que son emitidas por organizaciones acreditadas y validadas utilizando pruebas criptográficas. Emplea tecnología no interactiva de conocimiento-cero (zero-knowledge), concretamente zk-SNARK, para permitir la autenticación sin contraseña y la verificación global. Por último, dispone del MOI ID, un identificador descentralizado que identifica al poseedor de manera digital. La especificación de identidad descentralizada de MOI ID se basa en comportamientos humanos naturales y sostenibles para facilitar las interacciones digitales centradas en el participante.

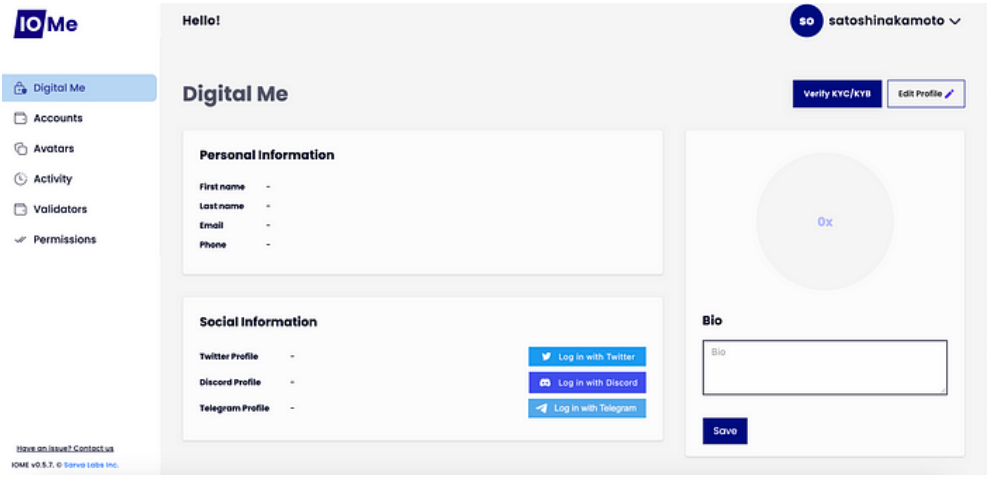


Ilustración 15 Interfaz aplicación IOME una vez el usuario se ha creado su MOI-ID

Para finalizar, cabe destacar el National Blockchain Project (PNB), una iniciativa del Ministerio de Electrónica y Tecnología de la Información (MeitY), anunciada en 2018, cuyo objetivo es aprovechar el potencial de la tecnología blockchain para impulsar la transformación digital del país. El PNB tiene como objetivos fomentar la innovación, mejorar la eficiencia y la transparencia, promover la inclusión financiera y fortalecer la seguridad cibernética.

3.3.2 Japón

Japón se encuentra en un proceso de transformación digital, y la identidad digital es un componente clave para esto. El gobierno ha implementado un

sistema de identificación digital conocido como “My Number”, que asigna un número único a cada residente. Aunque este sistema se ha enfrentado a distintos problemas técnicos, el gobierno está tomando medidas para mejorar el sistema. En cuanto a la tecnología Web3, el modelo japonés integra esta tecnología en la sociedad, resaltando principios altruistas y la gobernanza comunitaria. La influencia de la filosofía confuciana en Japón promueve la adopción de Web3, fomentando la armonía y el bienestar social, las estrictas regulaciones japonesas han contribuido a la aceptación de Web3, estas tecnologías han provocado el impulso de una economía de tokens y la promoción de modelos híbridos que combinan enfoques tradicionales con blockchain.

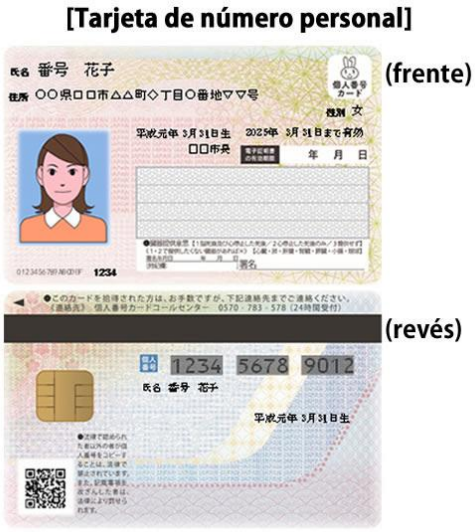


Ilustración 16 Tarjeta My Number

Mebuku Ground. Mebuku Ground Inc. es una empresa que está implantando un servicio de SSI en la ciudad de Maebashi, Japón. Además, de su arquitectura técnica, la empresa muestra gran importancia respecto a la gobernanza de los datos, priorizando los derechos de los consumidores sobre los derechos de propiedad económica de los inversores. Fue creada en octubre de 2022 como proveedor de servicios de identidad (IdP) y proveedor selectivo de tokens de atributos. Utiliza tecnología FPoS para generar pares de claves públicas y privadas en el teléfono móvil de los usuarios. Estos, tienen la opción de decidir qué atributos revelar a los proveedores de servicios, mientras mantienen otros atributos enmascarados. Las credenciales emitidas por Mebuku Ground están

vinculadas al sistema nacional de identificación digital "My number" de Japón. Actualmente hay 80 millones de tarjetas con identificación digital en manos de residentes japoneses. Al estar vinculado el Mebuku ID con el DNI nacional, se posibilita su utilización en transacciones sujetas a regulaciones contra el lavado de dinero. En caso de necesidad de rastrear a alguien por razones legales y de seguridad, se puede seguir un proceso democrático para acceder a la información en la identificación nacional. Los sistemas en funcionamiento en Mebuku Ground están tecnológicamente muy próximos al esquema eIDAS, ya que también ofrece una función de divulgación selectiva de atributos y pone énfasis en la construcción de relaciones confiables en las comunidades locales, mediante una estructura de gobernanza que incorpora un comité encargado del control de los datos.

Ilustración 17 Menú de inicio Mebuku

La empresa busca establecer un ambiente seguro para la transmisión de datos en la comunidad, para incentivar a las empresas privadas a proporcionar servicios críticos con información personal sensible. Un ejemplo pueden ser las alergias alimentarias, estas representan un desafío significativo en la crianza de los niños. Las escuelas de enfermería saben que simplificarían enormemente sus operaciones si hubiera un sistema para proporcionar a los proveedores de comidas información relevante sobre los requisitos alimenticios de cada niño.

Mebuku Ground permite esto emitiendo tokens al proveedor de alimentos, lo que facilita a las escuelas de enfermería compartir esta información de forma anónima. Aunque la decisión aún no se ha tomado, Mebuku Ground está considerando usar tecnología Web3 como una de las opciones.

3.3.3 Singapur

Singapur se encuentra en medio de un proceso de transformación digital del gobierno, con un gran enfoque en la eficiencia, la experiencia de usuario y la innovación. El gobierno de Singapur, a través de la Agencia de Tecnología (GovTech), está impulsando el Plan de Gobierno Digital (DGB), cuyo objetivo es transformar el sector público, a través de una digitalización responsable, repensando y rediseñando la forma en que el gobierno sirve a los ciudadanos, y sin olvidar que el sector público existe para servir a las personas.

Para facilitar la implementación del DGB, Singapur ha desarrollado la Pila de Tecnología del Gobierno de Singapur (SGTS). Esta pila es una infraestructura digital que permite construir servicios a escala, consta de almacenamiento en la nube, middleware y una biblioteca de microservicios para mejorar la interoperabilidad entre aplicaciones. Además, se está adoptando un enfoque centrado en el ciudadano, y en cómo las agencias gubernamentales les brindan servicios en torno a los trabajos que deben realizarse. Un ejemplo es la aplicación Moments of Life (Families), diseñada para padres con recién nacidos, esta aplicación simplifica tres tareas importantes: registrar el nacimiento y solicitar el bono de bebé, buscar instalaciones de preescolar y acceder a registros médicos del niño. Esta innovadora aplicación refleja la visión de transformar los servicios gubernamentales en torno a las necesidades específicas de los ciudadanos.

Para respaldar estas iniciativas, GovTech está transformando su cultura y capacidad internas para operar como un "nativo digital". Se han establecido equipos multidisciplinarios y se está fomentando un nuevo modelo de liderazgo colaborativo y ágil.

En medio de este contexto surgió un nuevo proyecto, **Singpass** [20] **,** una plataforma de verificación electrónica de identidad gestionada por el Gobierno de Singapur. Es la identidad digital que utilizan los residentes de Singapur para acceder de forma fácil y segura a más de 2700 servicios del gobierno y del sector privado, tanto en línea como en persona. Esta plataforma está gestionada por el GovTech y es uno de los ocho proyectos estratégicos nacionales, que impulsan la visión de nación inteligente de Singapur. Este proyecto se está teniendo una gran adopción, ya que actualmente más de 4,2 millones de personas utilizan Singpass app y se realizan más de 41 millones de transacciones por mes.

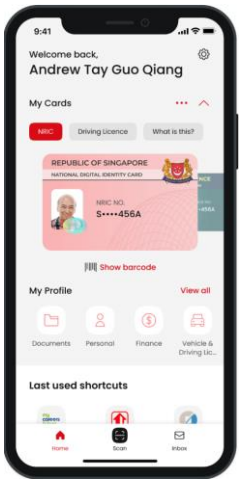


Ilustración 18 Singpass app

Singpass app fue lanzada en 2018 y las funciones actuales de la aplicación incluyen:

- Acceso con un solo toque a servicios digitales gubernamentales de uso común como CPF, HDB, IRAS y NS Portal. Los últimos servicios utilizados también se muestran para facilitar el acceso.
- Sección de perfil en la que los usuarios siempre tienen a mano su información importante, como el saldo del CPF y los datos del HDB.
- Prueba de identidad y suministro de información en persona, escaneando un código QR. Actualmente, los pacientes de las policlínicas SingHealth

[20] https://www.singpass.gov.sg/main

y los visitantes de Republic Plaza pueden utilizar su aplicación Singpass para registrarse, en lugar de rellenar formularios manualmente.

- Notificaciones puntuales de organismos públicos en la bandeja de entrada de la aplicación Singpass. Por ejemplo, los usuarios que deban renovar el NRIC y el pasaporte recibirán notificaciones en la bandeja de entrada de su aplicación.
- Firma digital de documentos mediante el escaneo de un código QR, lo que elimina la necesidad de que los usuarios estén fisicamente presentes para firmar documentos y acuerdos con empresas que ofrecen el servicio inicio de sesión con Singpass.
- Las personas autorizadas de entidades empresariales pueden cambiar a su perfil empresarial para acceder y ver datos corporativos seleccionados en la aplicación Singpass. Los usuarios deben tener una cuenta Corppass válida.

Por último, cabe destacar, que el gobierno de Singapur vino a España para visitar el consorcio de Alastria, y así ver su proyecto de identidad digital.

3.4 Oceanía

3.4.1 Australia

En Australia los principales proyectos de ley de identidad digital tienen su origen en la Investigación del Sistema Financiero de 2014. La investigación destacó que el enfoque dividido de la verificación de la identidad en Australia genera costes significativos para las personas, las empresas y la economía australiana en general. A través de esta investigación se recomendó desarrollar una estrategia nacional para un modelo federado de documentos de identidad digitales de confianza, en el que los proveedores de identidad de los sectores públicos y privados suministrarían documentos de identidad digitales, mejorando así la elección del consumidor, la privacidad y la eficiencia. Esto llevó al desarrollo del Marco de Identidad Digital Confiable y proporcionó elementos clave de la intención política que respaldan los proyectos de ley actuales. En 2016 se inició el marco de acreditación para promover un estándar nacional coherente para la identificación digital y establecer los requisitos de acreditación para los servicios de identificación digital que operan en el Sistema de

Identificación Digital del Gobierno de Australia. Con el paso del tiempo, han surgido gradualmente varios servicios de identificación digital. Australia Post lanzó su servicio Digital iD en 2017, mientras que myGovID, el proveedor de identificación digital del gobierno australiano fue lanzado en 2019. En los últimos veinte años, tanto gobiernos como organizaciones del sector privado en el ámbito internacional han implementado distintos servicios de identificación digital para facilitar y asegurar la verificación de la identidad de las personas al utilizar varios servicios.

El 30 de Noviembre de 2023 la Ministra de Finanzas, la Senadora Katy Gallagher, presentó en el Senado el **Digital ID Bill 2023**[21] y el Digital ID (Disposiciones Transitorias y Consecuenciales) Bill 2023 (el Proyecto de Ley Transitorio). El Digital ID es una forma cómoda y segura de verificar la identidad en línea y en persona. El proyecto de ley define la identificación digital como "una representación electrónica distinta de la persona que permite distinguirla suficientemente cuando interactúa en línea con los servicios". El proyecto no es un nuevo documento de identidad, ni un numero o identificador único para las personas, sino una arquitectura distribuida y federada que se crea verificando la información con documentos de identidad existentes emitidos por el gobierno, como el permiso de conducir, el pasaporte, etc. La creación de una identificación digital no centraliza la información personal y los datos en un solo lugar, al basarse en una arquitectura federada. Las personas pueden crear un Digital ID proporcionando una serie de datos asociados a la persona a un proveedor de identificación digital. La solidez del documento de Digital ID que una persona desea crear determinará el tipo y el número de atributos que deberá proporcionar a un proveedor de identificación digital. Pueden ser tres tipos:

- Identificación digital básica (Nivel de Verificación de Identidad 1) requiere una dirección de correo electrónico o número de teléfono móvil. Este se podría utilizar para reservar alojamiento para vacaciones o acceder a una

---

21 https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1404_first-senate/toc_pdf/2316120.pdf;fileType=application%2Fpdf

plataforma de streaming, donde verificar la identidad a un nivel alto no es necesario.

- Identificación digital estándar (Nivel de Verificación de Identidad 2) requiere dos documentos de identificación aceptables, como una licencia de conducir australiana, tarjeta de Medicare o certificado de nacimiento australiano. Este nivel de verificación podría ocurrir cuando alguien está configurando una nueva cuenta de servicios públicos o para ciertas transacciones financieras.
- Identificación digital fuerte (Nivel de Verificación de Identidad 3) requiere al menos dos documentos de identificación, uno de los cuales debe incluir una fotografía facial de la persona (por ejemplo, un pasaporte australiano). Además, se debe escanear el rostro con un teléfono. Este nivel también requiere un documento de "inicio de identidad", como una visa o certificado de nacimiento. Se utiliza frecuentemente al acceder a servicios gubernamentales en línea relacionados con el apoyo de ingresos.

Una vez que un proveedor de identificación digital ha recibido los atributos apropiados y los ha verificado, puede expedir a una persona una identificación digital.

El Sistema de Digital ID de Australia se encarga de que las personas verifiquen su identidad al gobierno y a las empresas de una manera segura y voluntaria. Este sistema consta de:

- El esquema de acreditación actual para servicios de identificación digital y el Esquema de Acreditación creado por el proyecto de ley de identificación digital (Digital ID Bill).
- El Sistema de Identificación Digital del Gobierno Australiano, que será legislado a través del proyecto de ley de identificación digital y que actualmente permite a las personas utilizar una identificación digital en una variedad de servicios gubernamentales.

El esquema actual de acreditación establece normas para los proveedores de servicios de identificación digital que ya están acreditados en el sistema, incluidos aquellos que funcionan dentro del Sistema de Identificación Digital del Gobierno Australiano. Este esquema establece requisitos para asegurar la

seguridad y facilidad de uso de los servicios, tratando temas como accesibilidad, protección de la privacidad, control de seguridad y fraude, gestión de riesgos e interoperabilidad técnica. Desde que comenzó en 2016, el plan ha sido modificado seis veces para mantener su importancia y mejorar la privacidad y la seguridad en línea con las cambiantes necesidades.

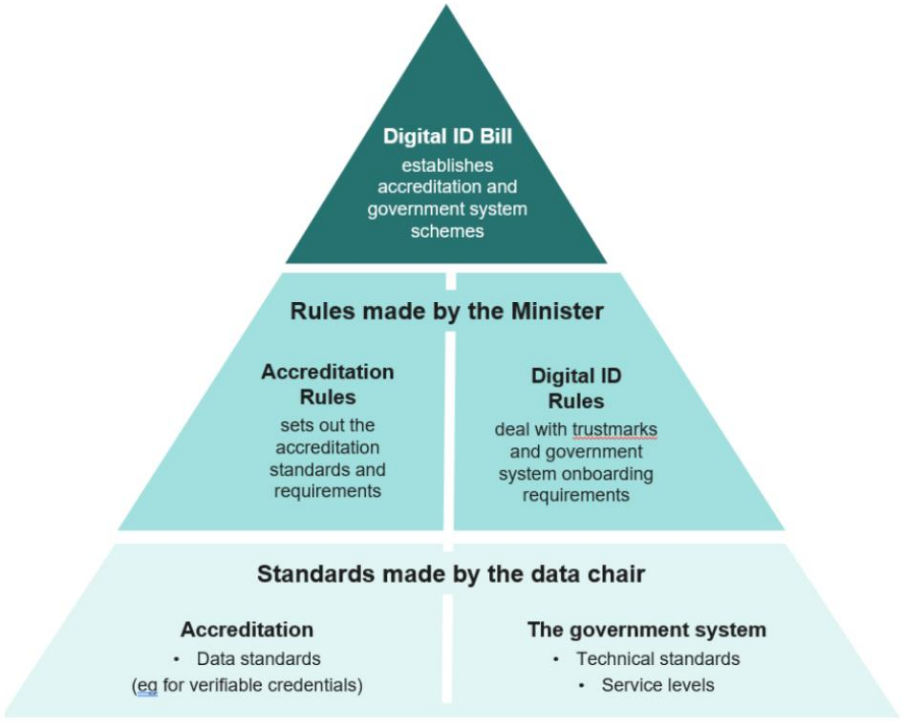


Ilustración 19 Structure of the legislative framework

El Sistema de Identificación Digital del Gobierno Australiano actualmente cuenta con más de 10.5 millones de identificaciones digitales creadas a través del proveedor de identificación digital del gobierno, myGovID. Esta plataforma permite el acceso a más de 130 servicios gubernamentales tanto a nivel federal como estatal y territorial. Este sistema que al principio se centraba en los servicios del Commonwealth (servicios ofrecidos por el gobierno federal o nacional, que abarcan áreas como impuestos, asuntos de inmigración, seguridad social y otros servicios de ámbito nacional), ahora ha crecido para abarcar también los servicios gubernamentales estatales y territoriales. Los servicios actuales pueden utilizar el nuevo marco legal establecido por la Ley de Identificación Digital a través del Proyecto de Ley Transitorio y sus reglamentos correspondientes.

myGov es una plataforma gubernamental que ofrece acceso seguro a una gran variedad de servicios en línea desde un único lugar. Tanto la página web de myGov como la app myGov posibilitan el acceso a la cuenta del usuario. Por otro lado, myGovID es una app de identidad digital del gobierno australiano. El objetivo de esta es que los usuarios puedan demostrar de manera segura su identidad al acceder a servicios gubernamentales en línea. Los usuarios pueden enlazar su myGovID a su cuenta de myGov para hacer más sencillo el acceso a estos servicios.

ConnectID[22] es una solución de identidad digital de propiedad australiana que facilita el intercambio de datos y permite a las empresas verificar de forma sencilla y segura la identidad de sus clientes. ConnectID puede integrarse con los sistemas y plataformas existentes. Está acreditado por el Trusted Digital Identity Framework (TDIF) del Gobierno australiano y se ha creado conforme a las normas establecidas por el Gobierno australiano, lo que implica que los datos de los clientes están seguros y protegidos. ConnectID es una iniciativa de Australian Payments Plus (AP+). AP+ reúne a eftpos, BPAY y NPP Australia en una única organización para dar forma al futuro de los pagos. Este proyecto se comenzó a implantar en Australia en 2023.

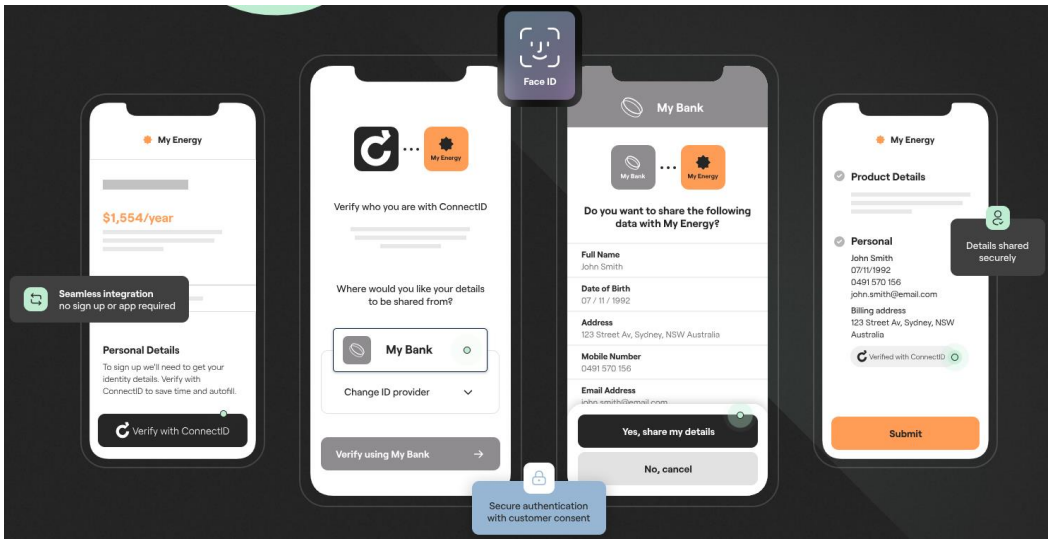


Ilustración 20 ConnectID caso de uso

[22] https://connectid.com.au/

3.5 Europa

3.5.1 España

España, ha sido uno de los países pioneros en emplear soluciones descentralizadas basadas en tecnología blockchain para la gestión de identidad digital. El primer acercamiento a la identidad digital fue la implantación del DNI electrónico en 2006, esta es, actualmente, la herramienta principal de identificación digital, la cual permite la firma electrónica y el acceso a tramites online. Es país ha ido evolucionando hacia la creación de iniciativas de redes blockchain para identidades digitales, como puede ser Alastria, de esta forma, España, se ha ganado el reconocimiento internacional, lo que le ha permitido participar en iniciativas de la Unión Europea para promover el uso de la tecnología blockchain para la gestión de identidades digitales. Por todo esto España lidera la exploración del modelo SSI, con el objetivo de seguir desarrollando y promoviendo soluciones SSI descentralizadas, basadas en blockchain, para mejorar la seguridad, privacidad y el control de los ciudadanos sobre sus datos.

Ilustración 21 Nuevo logotipo de Alastria

Alastria se define como "una asociación sin ánimo de lucro que tiene como objetivo fundamental crear una comunidad integrada por todo tipo de organizaciones públicas y privadas, así como expertos individuales, para favorecer la implantación, estandarización, protección y utilización de las tecnologías tipo Distributed Ledger Technologies (DLT), fomentando el conocimiento y el uso por la sociedad española de esta tecnología, promoviendo su uso entre las administraciones, las empresas y demás agentes sociales".

Alastria es una plataforma público-permisionada, de propósito general, alineada con la regulación y orientada a soportar casos de uso de múltiples industrias. El modelo de consenso es Proof of Authority (PoA), este mecanismo

confía en la verificación de las identidades para validar las transacciones y crear nuevos bloques. Algunos de los objetivos de Alastria son democratizar el acceso a la tecnología blockchain, fortaleces el ecosistema blockchain, fomentar nuevos modelos de negocio de economía digital, facilitar el desarrollo de tecnologías blockchain y fomentar el conocimiento de blockchain potenciando así los casos de uso para el mundo real.

Alastria ID

Alastria ID es un modelo de identidad digital creado por el consorcio de blockchain español, Alastria. Este proyecto sigue el incipiente modelo de identidad, Self Sovereign Identity (SSI) y tiene como objetivo proporcionar una identidad digital a los usuarios para que la puedan utilizar para todo tipo de transacciones en línea como puede ser abrir una cuenta bancaria, de forma segura y con control de sus datos, pagar impuestos, alquilar artículos etc.

Alastria ID se construye sobre la red de Ethereum. A su vez, existen dos redes distintas a través de la cuales los socios pueden desplegar sus nodos. Hay dos redes debido a que los socios no quieren tener que confiar en una única plataforma. Esto proporciona beneficios como adaptación, ya que diferentes redes pueden tener capacidades que se adapten mejor a diferentes situaciones, y también mayor seguridad, ya que algunos protocolos de blockchain pueden no prosperar, perdiendo así su soporte. Estas dos redes, clientes de Ethereum, son:

- RED T: Es la red basada en tecnología Quórum. Se trata de una red robusta, estable y con alta resiliencia. Esta desplegado sobre la red global de centros de datos de Microsoft Azure.
- RED B: Es la red basada en la tecnología Hyperledger Besu. Se trata de una red moderna y potente con la misma tecnología utilizada por la red europea EBSI y la red latinoamericana LACCHAIN.

Este proyecto de basa en los 10 principios clave de SSI, algunos de los cuales desarrollamos en el punto 2.1.1. Estos 10 principios los podemos agrupar en tres pilares: Seguridad, controlabilidad y portabilidad.

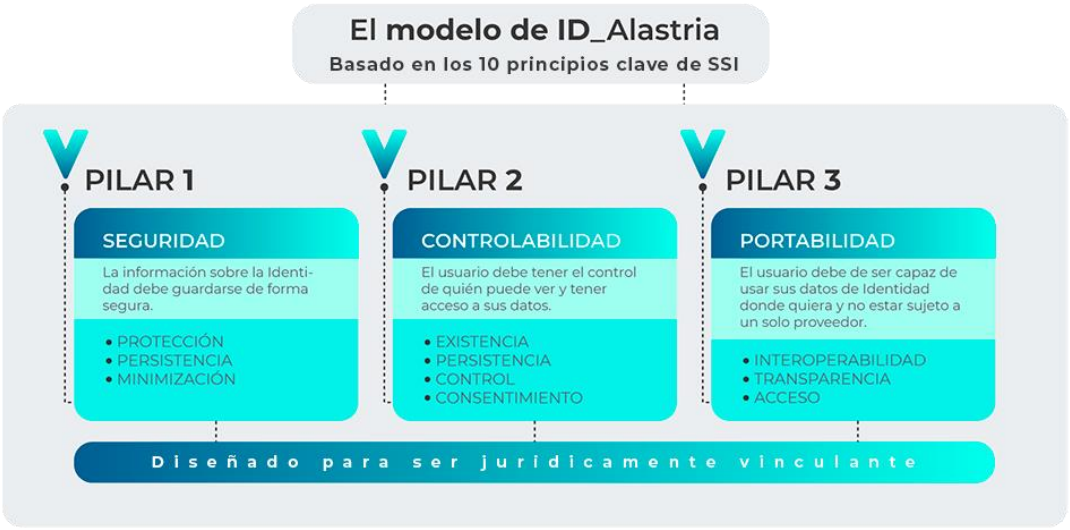


Ilustración 22 Los tres pilares de AlastriaID

Se trata de un modelo open source que ha sido construido colaborativamente por los miembros del consorcio. Este se encuentra en constante proceso de revisión y testeo para mejorar la seguridad y privacidad, todo ello alineado con la normativa española y europea. Este modelo permite al usuario gestionar sus datos desde sus dispositivos, de forma segura, fiable y transparente. Alastria ID implementa Smart contracts (contratos inteligentes) y componentes software, lo que permite que se integren con backends de distintos servicios. Todo esto se coordina gracias al protocolo definido por parte del modelo y gracias a la wallet, una aplicación desde la cual, los usuarios tendrán control total sobre los datos compartidos, con quién se comparten y durante cuánto tiempo. También podrán ejercer sus derechos definidos por el GDPR, borrando o cancelando los datos que deseen.

Por último, cabe destacar que Alastria ID es un referente global en identidad digital, ya que este modelo ha servido de base para la publicación de la "Norma UNE 71307-1", el primer estándar global sobre gestión de identidades digitales descentralizadas basado en Blockchain y Tecnologías de Registro Distribuido (DLT). Además, este modelo se ha adoptado como referencia en documentos elaborados por organismos internacionales de normalización como ISO e ITU.

Dalion es un proyecto que surgió en 2019, con el objetivo de crear una solución de identidad digital autogestionada, permitiendo así a los usuarios un control

completo de sus datos. El proyecto tiene como objetivo aplicar el modelo de identidad de Alastria incorporándolo en las aplicaciones y procesos ya existentes. Inetum coordina este proyecto junto a otras empresas y entidades académicas: la Universidad Politécnica de Madrid, MAPFRE, Banca March, Generali, Banco Santander, BBVA, CaixaBank, Línea Directa Aseguradora, Unicaja Banco y Repsol.

Este proyecto está basado en el modelo Alastria ID y en el estándar UNE 71307. A través de este modelo el usuario puede controlar con quién, para qué y hasta cuando comparte sus datos, de una manera rápida, sencilla y segura. Esto tiene grandes beneficios ya que una vez los datos del usuario sean validados por distintas entidades, este los podrá utilizar para pedir un préstamo, dar de alta el servicio de luz o gas, alquilar un coche etc. Además, gracias a la tecnología blockchain, se facilita al emisor la firma de credenciales y su posterior revocación en caso de necesidad, cumpliendo así con uno de los derechos fundamentales registrados en el RGPD.

Todo este control completo de datos, el usuario lo gestionará a través de una wallet digital, donde el usuario podrá acceder a todas sus credenciales, gestionándolas a su conveniencia, además de identificarse y autenticarse ante cualquier sitio web o aplicación móvil que utilice el sistema. Gracias a esta wallet, además de tener el registro de todos los datos presentados, el usuario podrá solicitar al proveedor de servicios, que deje de utilizar sus datos, a través de un simple “click”.

Los valores diferenciales que identifica la asociación Alastria para este proyecto son: multisectorial, múltiples casos de uso, interoperabilidad, sandbox financier y colaboración público-privada.

Ilustración 23 Domiciliación de un recibo. Dalion

3.5.2 Resto de Europa

En los últimos años, el concepto de identidad digital autogestionada (SSI) ha experimentado un notable aumento en el contexto europeo actual. Frente al creciente aumento de la importancia de SSI, Europa respondió con la implementación de una nueva regulación para este nuevo paradigma, el Reglamento Nº 910/2014 del Parlamento Europeo y del Consejo, conocido como el Reglamento de Identificación Electrónica (elDAS). Esta legislación establece un marco normativo integral para la identificación electrónica, la autenticación y los servicios de confianza dentro del mercado interno europeo.

eIDAS ha logrado un avance significativo en el ámbito legal de la Unión Europea, a través de la iniciativa de crear confianza en las transacciones en línea y de promover la adopción de la identidad digital. También incluye disposiciones para la validación transfronteriza de los sistemas de identificación electrónica. Para que un sistema así sea válido legalmente en un entorno transfronterizo, deberá satisfacer algunos criterios como incluirse en una lista oficial publicada por la Comisión Europea y asegurar un nivel significativo o alto de seguridad. Este reglamento también ha sigo responsable del gran avance que ha tenido la identidad autogestionada en Europa, además de ser el responsable de establecer las bases regulatorias.

Ilustración 24 eIDAS

En medio de este contexto, nació en 2018 la European Blockchain Servicies Infrastructure (**EBSI**), cuando todos los estados miembros de la UE, Noruega y Liechtenstein (29 países) y la Comisión Europea se unieron para crear la European Blockchain Partnership (EBP). El objetivo de la EBP es utilizar la tecnología blockchain para crear servicios transfronterizos destinados a las administraciones públicas, las empresas, los ciudadanos y sus ecosistemas para verificar la información y hacer que los servicios sean fiables. EBSI es la primera iniciativa paneuropea de blockchain y consiste en una red peer-to-peer de nodos interconectados que ejecutan una infraestructura de servicios basada en blockchain. La infraestructura tiene distintas capas: una capa con la infraestructura básica, la conectividad, la cadena de bloques y el almacenamiento necesario, una capa de servicios básicos que permitirá usar y aplicaciones basadas en EBSI y, por último, las capas adicionales dedicadas a uso y aplicaciones específicas. Esta red aprovecha las propiedades descentralizadas, inmutables y a prueba de manipulaciones de blockchain para respaldar mejores servicios públicos para toda Europa. Los tres pilares de EBSI son:

- Negocios: ¿Qué se puede hacer con EBSI?
  EBSI ofrece una gran variedad oportunidades para distintos sectores e industrias utilizando tecnología blockchain. Estas oportunidades se agrupan en “Familias de casos de uso”, que representan distintas áreas temáticas donde EBSI puede proporcionar soluciones para múltiples campos, por ejemplo, "Track & Trace" para trazabilidad, "credenciales verificables" para verificación, etc.
- Tecnología: ¿Cómo funciona?
  El funcionamiento de EBSI se basa en tres componentes principales. Las API, los contratos inteligentes y el libro mayor. Las API, son accesibles a través del internet público, y sirven de interfaz para que las aplicaciones

interactúen con EBSI, facilitando así la recuperación de datos y la ejecución de transacciones. Los contratos inteligentes funcionan como acuerdos digitales, se activan mediante solicitudes de API para llevar a cabo las tareas predefinidas y garantizar así que las transacciones se registran de forma segura en el libro mayor. Por último, el libro mayor es una base de datos descentralizada, organizada en bloques interconectados donde se registran las transacciones de manera inmutable, proporcionando así confianza.

Así, un actor realiza una operación comercial, incluida en uno de los casos de uso de EBSI, usando una aplicación para conectarse a una de las API de EBSI. Lee la información almacenada en el libro mayor o registra una transacción, después, en función de la solicitud del usuario, la API llama a un contrato inteligente que realizará la operación y la registrará en el libro mayor, completando así el flujo de datos.

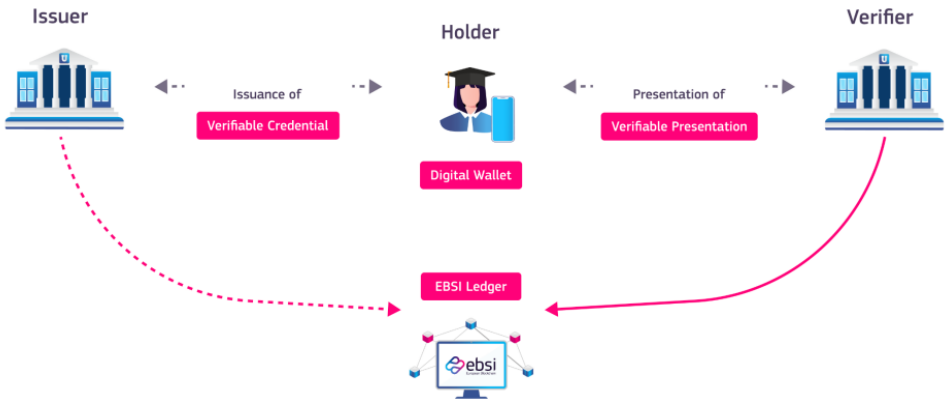


Ilustración 25 Flujos de datos EBSI

- Infraestructura: una red paneuropea de nodos

  EBSI es una red de nodos repartidos en Europa donde se alojan de manera descentralizada lo principales servicios técnico (API, contratos inteligentes y el libro mayor). Estos nodos sincronizan las copias del libro mayor y lo distribuyen, poniendo a disposición los servicios técnicos básicos de EBSI. Cualquiera puede optar por operar un Nodo EBSI, pero los Operadores de Nodos deben cumplir con las reglas de Gobernanza de EBSI y respetar sus Condiciones Generales para Operadores de Nodos para garantizar la integridad y estabilidad de la red. Estos Operadores de nodos están aprobador por la EBP.

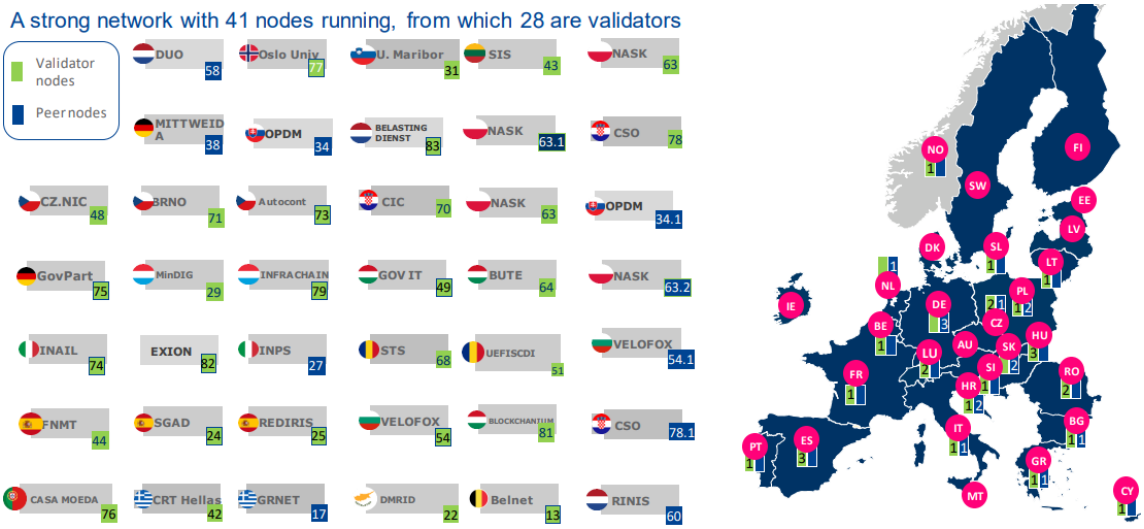


Ilustración 26 Operadores de nodos en la red piloto EBSI

Respecto a los niveles de seguridad (LoA), se definen en el el Articulo 8[23] - "Assurance levels of electronic identification schemes" del eIDAS Regulation, tres niveles de seguridad para la emisión de credenciales verificables: bajo, sustancial y alto. Estos niveles determinan los requisitos de autenticación y verificación de identidad que deben cumplirse para emitir una credencial con un determinado nivel de confianza.

- Nivel Bajo (Low): Se utiliza para credenciales de bajo riesgo y se basa en la autenticación mediante contraseña o mecanismos similares.
- Nivel Sustancial (Substantial): Implica una autenticación más robusta, como la autenticación de dos factores o la verificación remota de identidad.
- Nivel Alto (High): Requiere la verificación presencial de la identidad y una autenticación reforzada, como el uso de tokens criptográficos.

Estos últimos años se ha estado trabajando en una nueva actualización del reglamento europeo eIDAS, dando lugar al reglamento eIDAS2, aprobado el 29 de Febrero de 2024 por el Parlamento Europeo. eIDAS2 es una revisión del Reglamento Nº 910/2014 sobre identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interno europeo.

[23] https://www.eid.as/#article8

En **eIDAS2** se introducen nuevos tipos de credenciales, como las credenciales verificables. Estas permiten a los usuarios demostrar y compartir sus datos sin revelar información personal innecesaria. Estas nuevas credenciales surgen debido a la nueva normativa, en cuanto a la gestión de identidad digital, ya que abarca no solo la identificación y autenticación, sino también cualquier otro detalle o característica de los ciudadanos que pueda requerir certificación, por ejemplo, número de la seguridad social, ser titular de una cuenta bancaria, títulos universitarios etc. Se facilita la interoperabilidad transfronteriza de los servicios de confianza. Los distintos campos de aplicación de casos de usos aumentan, llegando a sectores como la salud, la movilidad o la educación. Se introduce un nuevo nivel de seguridad, el cuarto, nivel de seguridad "muy alto", para las transacciones de alto riesgo. Por último, se refuerza la seguridad de la identificación electrónica y los servicios de confianza dando nuevos métodos de identificación y autenticación, todo esto a través de la nueva EUDI Wallet (EDIW).

Ilustración 27 Ejemplo de uso de EUDI Wallet

La **EDIW**, es una cartera digital y se define como un medio de identificación, que permite almacenar datos de identidad y declaraciones electrónicas de atributos, así como crear firmas electrónicas. Contiene por tanto datos de identificación personal (PID) que permiten la identificación a nivel alto, cuya gestión está reservada a los estados miembros. Esta cartera debe ser gratuita para los usuarios, debe soportar el uso presencial y el uso a distancia, debe realizar la autenticación del tercero que solicite datos y debe soportar el uso entre particulares. También permitirá a los usuarios identificarse y autenticarse en línea, firmar documentos electrónicos de forma segura con firma electrónica cualificada directamente desde la EDIW, la creación de seudónimos para proteger la privacidad al acceder a servicios online y, finalmente, acceder a servicios públicos y privados de forma segura.

El ciudadano usará esta cartera de forma completamente voluntaria, en cambio, las grandes empresas y las administraciones públicas que requieran autenticación o identificación estarán obligadas a aceptar su uso a petición del usuario. Todos los estados miembros están obligados a que sus ciudadanos dispongan de al menos una EDIW para el tercer trimestre de 2026.

4 Análisis compatibilidad Alastria y EBSI

4.1 Análisis del funcionamiento

Creación de un id en Alastria

El proceso de creación de un Alastria ID comienza cuando un nuevo usuario accede al sitio web de una entidad emisora de credenciales. El usuario debe haberse registrado previamente para obtener un Legacy ID en dicha entidad. Una vez que el usuario ha iniciado sesión en el sitio web, aparece la opción de crear un Alastria ID, a través del despliegue de un código QR en la pantalla. Este código QR contiene un Alastria Token firmado por la entidad con su clave privada. El usuario escanea este código QR utilizando una aplicación wallet instalada en su teléfono (si el usuario no tiene una wallet en su teléfono, le aparecerá un código QR para descargarla ya sea en Android como iOS).

Tras escanear el código QR, la aplicación wallet, verifica la identidad de la entidad utilizando el DID del Alastria Token y obtiene su clave pública en el Smart Contract AlastriaPublicKeyRegistry. Este paso es muy importante para garantizar la autenticidad de la entidad y la seguridad del proceso. Una vez que la identidad de la entidad ha sido verificada, la aplicación wallet verifica la validez de todos los campos del Alastria Token. Si todos los campos son válidos, la wallet crea un artefacto de tipo Alastria Identity Creation. Este artefacto contiene el Alastria Token recibido, la transacción createAlastriaTX y la clave pública del usuario, todos ellos firmados por la clave privada del usuario. Una vez creado este artefacto, la entidad emisora de credenciales lo recibe (el AIC, Alastria Identity Creation) y verifica la procedencia del token utilizando la clave pública del usuario. Luego, la entidad realiza las transacciones prepareAlastriaID y createAlastriaID en el Smart Contract AlastriaIdentityManager, generando así el despliegue de un nuevo Alastria Proxy que contiene el DID del nuevo usuario, enlazándolo con el EOA del usuario. Finalmente, la clave pública del usuario se registra en el AlastriaPublicKeyRegistry vinculada a su DID. Además, la entidad asocia el DID generado al Legacy ID del usuario desde su Backend. Una vez terminado todo esto, el Alastria ID está creado.

Creación de un id en EBSI

A continuación, vamos a desglosar el proceso de creación de un id en 4 partes:

1. Generación de pares de claves: El paso inicial en la creación de una identidad digital EBSI es la generación de un par de claves criptográficas. Este par consta de una clave pública y otra privada. La clave privada se almacena de forma segura en una cartera digital y sólo puede acceder a ella el propietario.
2. Creación del DID: Con el par de claves, se crea un Identificador Descentralizado (DID). Este DID actúa como identificador único en el ecosistema EBSI. El documento DID, que incluye la clave pública y otros metadatos relacionados con la identidad, se registra a continuación en la blockchain EBSI con el equipo de apoyo.
3. Verificación de identidad: Una vez el DID está asociado a una clave privada, se procede a la verificación de identidad. Esto puede implicar proporcionar información o documentos personales adicionales, o utilizar un servicio de verificación de identidad seguro.
4. Finalmente, ya estaría creado el ID, que puede usarse para acceder a aplicaciones y servicios habilitados para EBSI.

Como en la página oficial de EBSI ni en su repositorio oficial he encontrado información sobre el proceso, esta información la redacté en base a una respuesta recibida por el equipo de apoyo de EBSI. Me registré una cuenta en EU Login, para así poder enviar un mail solicitando información al equipo de apoyo.

Emisión de una credencial en Alastria

Primeramente, el usuario accede a la página web de la entidad emisora de credenciales, iniciando sesión con su correspondiente Alastria ID. Una vez iniciada sesión, el usuario selecciona la credencial, la cual contiene información verificada por la entidad, que quiere que sea emitida. A la par que aparece en la web un código QR con la credencial firmada, se guarda en el Smart Contract AlastriaCredentialRegistry un PSMHash generado con la credencial y el DID de la Entidad Emisora de Credenciales. Este PSMHash se utiliza para certificar que la credencial ha sido emitida y permite que la entidad controle su estado de

validez. El usuario escanea el código QR generado, a través de su aplicación wallet, y verifica la credencial. Después de esto, la aplicación wallet muestra las credenciales solicitadas junto a un botón para que el usuario termine de confirmar la aceptación de estas credenciales. Al aceptarlas, se registra un nuevo PSMHash en el AlastriaCredentialRegistry. Este nuevo PSMHash, formado por la credencial y el DID del usuario, indica que el usuario ha aceptado estas credenciales y le permite controlar su estado.

Finalmente, ya estaría emitida la credencial.

Emisión de una credencial en EBSI

Como aclaro en las conclusiones, el repositorio de EBSI no tiene información precisa sobre este proceso, no presenta diagramas UML ni información técnica del funcionamiento, por lo tanto, en función de lo que he leído mi análisis de funcionamiento es el siguiente:

Para mejorar el control del titular sobre sus datos, surgió un nuevo modelo de intercambio de información. Este nuevo modelo de intercambio de información autónomo en tres pasos permite a los titulares compartir su información con quien quieran. EBSI seleccionó OpenID para protocolos de credenciales verificables.

OpenID para VC (OID4VC) es un protocolo que admite el intercambio de credenciales autónomo donde el titular puede controlar de forma autónoma el intercambio de credenciales con cualquier verificador que desee. Este se compone de tres estándares.

- En cuanto a la autenticación utiliza SIOPv2. Define como los titulares pueden autenticarse de manera autónoma con cualquier actor. (EBSI admite cualquier otra autenticación y no se limita a SIOPv2 para autenticación del titular)
- En cuanto a la emisión utiliza OID4VCI (OpenID for Verifiable Credential Issuance): Define las API y los correspondientes mecanismos de autorización basados en OAuth2 para la emisión de Credenciales Verificables.

- En cuanto a la presentación utiliza OID4VP (OpenID for Verifiable Presentations): Define mecanismos además de OAuth2 para permitir la presentación de reclamos en forma de Credenciales Verificables.

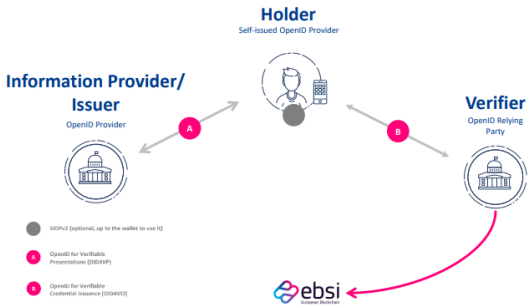


Ilustración 28 Vista simplificada con los tres estándares.

Funcionamiento de OpenID para la emisión de credenciales verificables:

1. Solicitar la credencial verificable.
   Un titular inicia la emisión en el sitio web del emisor, y la cartera digital (wallet) recibe información sobre el tipo de Credencial Verificable solicitada por el titular mediante un código QR o una redirección a la wallet. Este paso se omite si el usuario solicita la VC a la wallet. La wallet obtiene los metadatos del emisor para conocer los flujos, formatos, firmas y puntos finales admitidos. OID4VCI amplía los metadatos de OAuth2. La wallet solicita una credencial verificable. La solicitud de autorización es una solicitud de autorización OAuth2 ampliada en la que la wallet puede definir el tipo y formato de la VC y el tipo y formato de la firma.
2. Autenticación. El titular se autentica con el emisor mediante el método de autenticación admitido por el emisor.
3. Emisión de la credencial verificable. Tras una autenticación correcta, la wallet recibe un código OAuth2 que envía al punto final de token OAuth2 para recibir un token de acceso y una prueba para demostrar el control de la clave DID. El emisor devuelve un token de acceso y una prueba que se le pide que firme. El titular tiene que firmar la prueba con su(s) clave(s) DID para demostrar el control de las claves DID.
4. Obtención de la credencial verificable. El emisor emite un VC y notifica a la billetera donde se almacena.

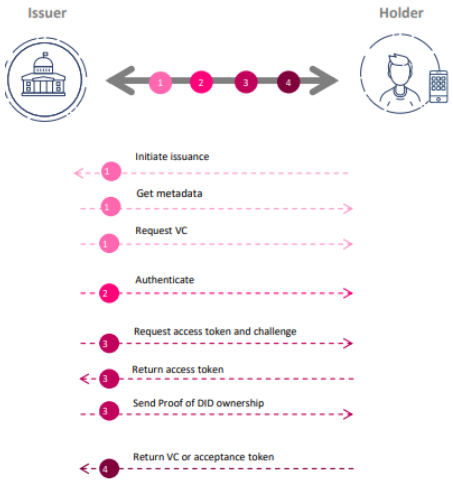


Ilustración 29 Emisión credencial verificable EBSI.

Reglamento General de Protección de Datos

Como hemos visto en los primeros capítulos, una de las principales características de la blockchain es su inmutabilidad, debido a que cada bloque referencia al anterior, formando así una cadena de bloques. Para alterar la información en un bloque se requeriría cambiar la referencia del siguiente, y, por ende, de todos los bloques sucesivos, por lo que cuanto más bloques tenga la cadena, más inmutable se vuelve.

Esta inmutabilidad se vuelve un problema a la hora de ejercer el derecho a la rectificación o el derecho a supresión de los datos del Reglamento General de Protección de Datos. Esto implica que las credenciales cuya información se almacena directamente en la cadena no cumplen con esta regulación. Una solución propuesta es cifrar la información antes de escribirla en la cadena de bloques, pero no todas las técnicas para ocultar la identidad son adecuadas según el RGPD, ya que deben cumplir ciertas características: no se obtiene el dato original solo a partir del dato cifrado. La clave en el cifrado hash puede proporcionar esta característica, además, facilita la eliminación de la información de la cadena y borrar la clave. Esto asegura que la información almacenada en la cadena sea imposible de recuperar a partir del dato original, cumpliendo así con el RGPD. En caso de modificación, se crearía un nuevo token con una nueva clave y resumen hash bajo el mismo protocolo, lo que

permite seguir cumpliendo con el RGPD, aunque se utilice una estructura descentralizada para los DIDs.

Revocación de una credencial en Alastria

En Alastria, las credenciales emitidas y las presentaciones realizadas, pueden ser revocadas tanto por la entidad emisora como por el usuario propietario, permitiendo así que en caso de presentar información a una entidad y luego no desear que esta la utilice, el usuario pueda revocar la presentación.

El usuario únicamente tendría que acceder a su wallet personal y seleccionar las credenciales que quiere revocar y cambia su estado. De esta forma lo que ocurre es que la credencial se elimina del AlastriaCredentialRegistry o la presentación del AlastriaPresentationRegistry.

Para finalizar, cabe destacar que Alastria no registra las credenciales en la blockchain, sino que utiliza un mecanismo de escritura, para registrar el estado de la credencial como revocada, en la blockchain. La credencial emitida, salvo que la entidad lo pida expresamente, no se graba en la blockchain, de todas formas, si se registra una credencial en la blockchain, lo que se escribe es el hash de la credencial, nunca se escriben los datos directamente en la blockchain.

Revocación de una credencial en EBSI

En cuanto a EBSI, existe un marco de Estado de Credencial, este permite a los emisores tener un control detallado sobre la vida útil de las credenciales que emiten. Este marco debe incluir parámetros que determinan la validez de las claves públicas y el estado actual de la VC (válido, revocado o suspendido). La revocación y la suspensión siguen un proceso similar, siendo la suspensión temporal y reversible, mientras que la revocación es permanente e irreversible.

Es importante saber que EBSI funciona a través de llamadas a API's y que las credenciales verificables dependen de tres componentes clave: las propiedades inherentes de la VC, la autenticidad de las claves públicas utilizadas para firmar/sellar la VC y su estado actual (válido, revocado o suspendido).

Hasta donde llega la información oficial de la página web de EBSI, para cambiar el estado de una VC de válida a revocada, hay que hacer una llamada a una API

que se realice este proceso, pero en la documentación de la API's no aparece dicha llamada para realizar el cambio, por lo que no podemos afirmar con total certeza que este método se esté aplicando.

4.2 Diseño diagramas de secuencia propios

A continuación, se mostrarán los diagramas de secuencia realizados para este análisis, para los procesos de creación de un identificador y para los procesos de emisión de credenciales en Alastria y en EBSI, y, por último, para el proceso de revocación de credenciales en Alastria.

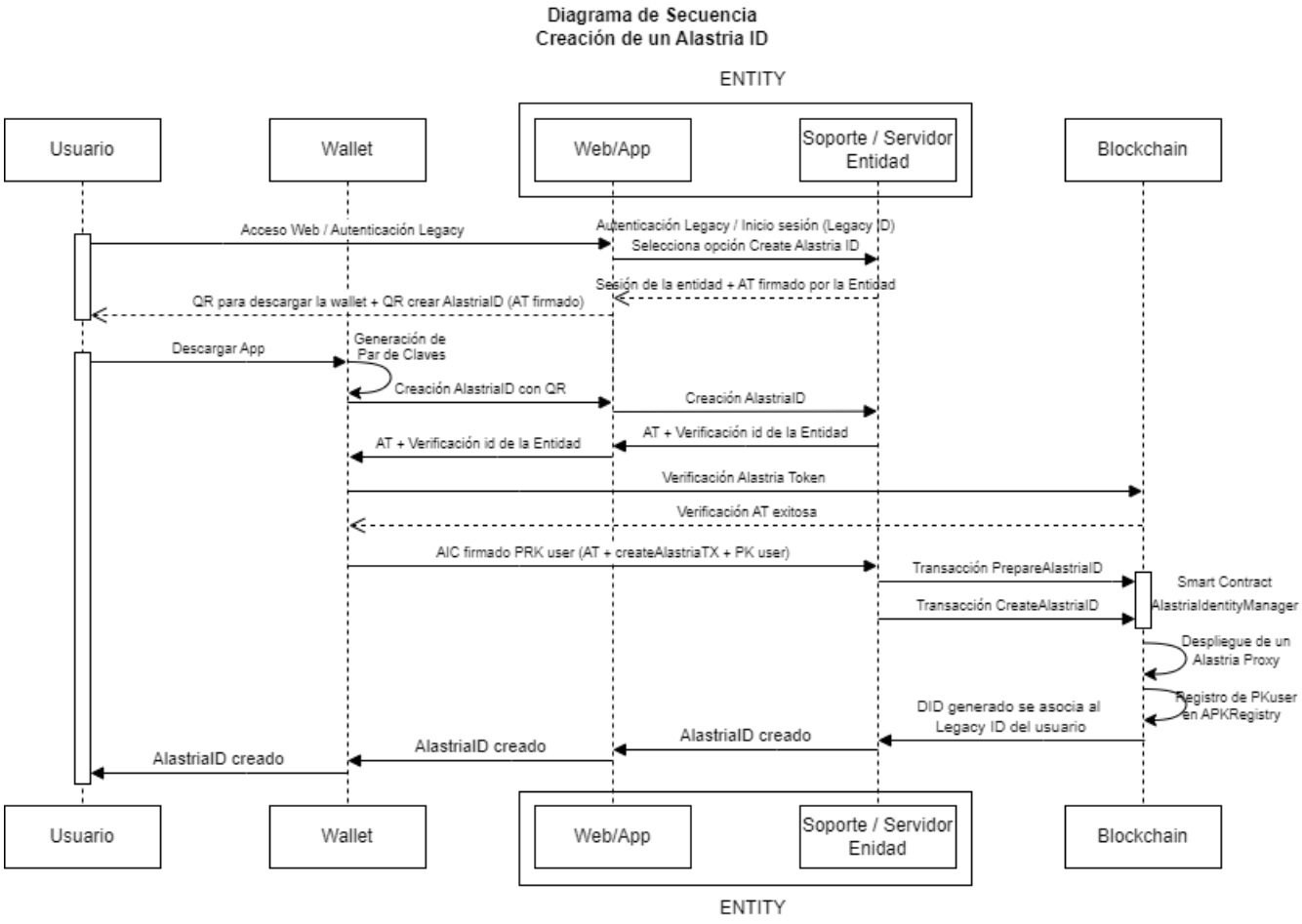


Ilustración 30 Diagrama de Secuencia Creación de un ID en Alastria

En el **Anexo** se detallarán los pasos que forman parte de los distintos diagramas de secuencia.

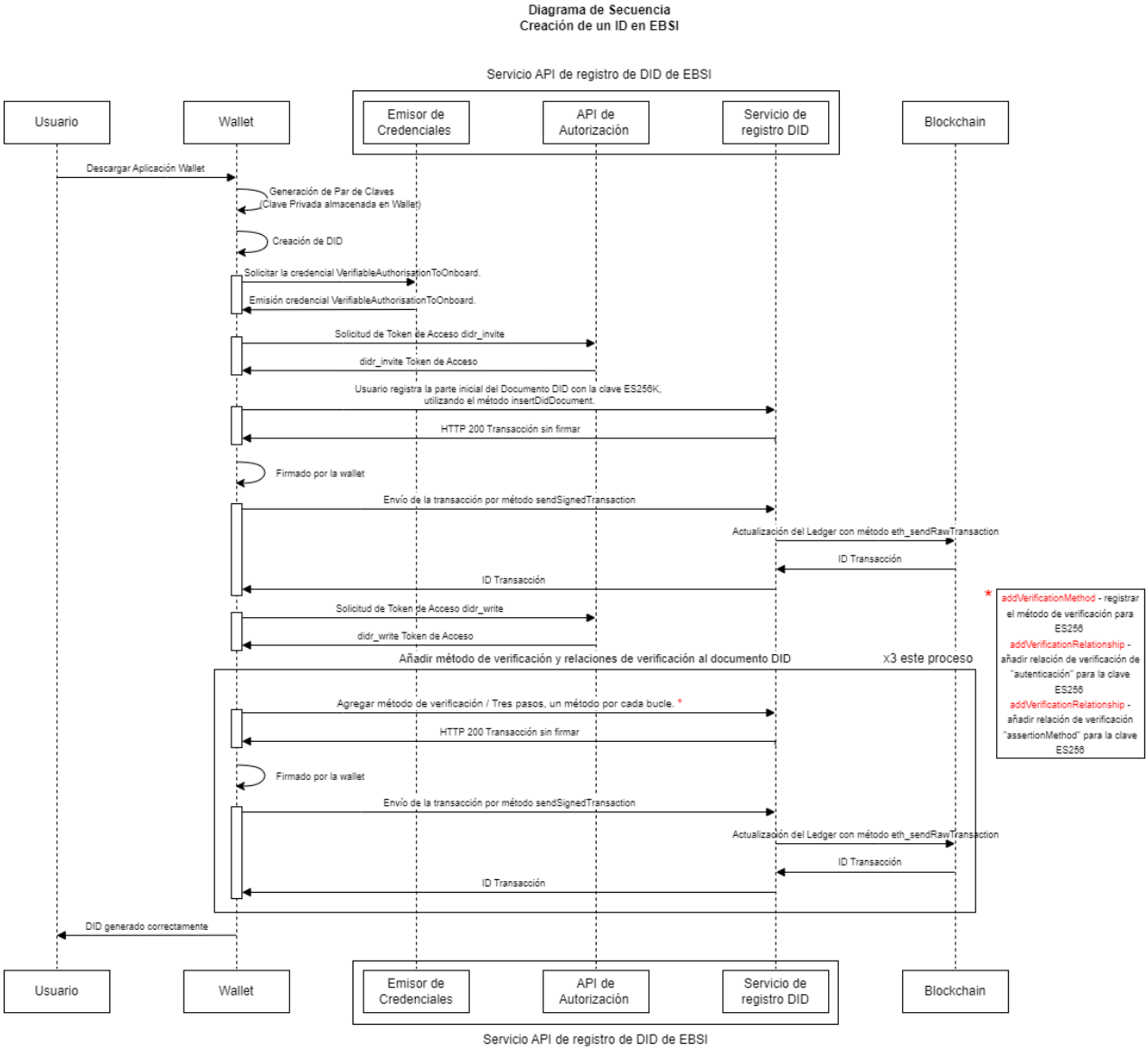


Ilustración 31 Diagrama de Secuencia Creación de un ID en EBSI

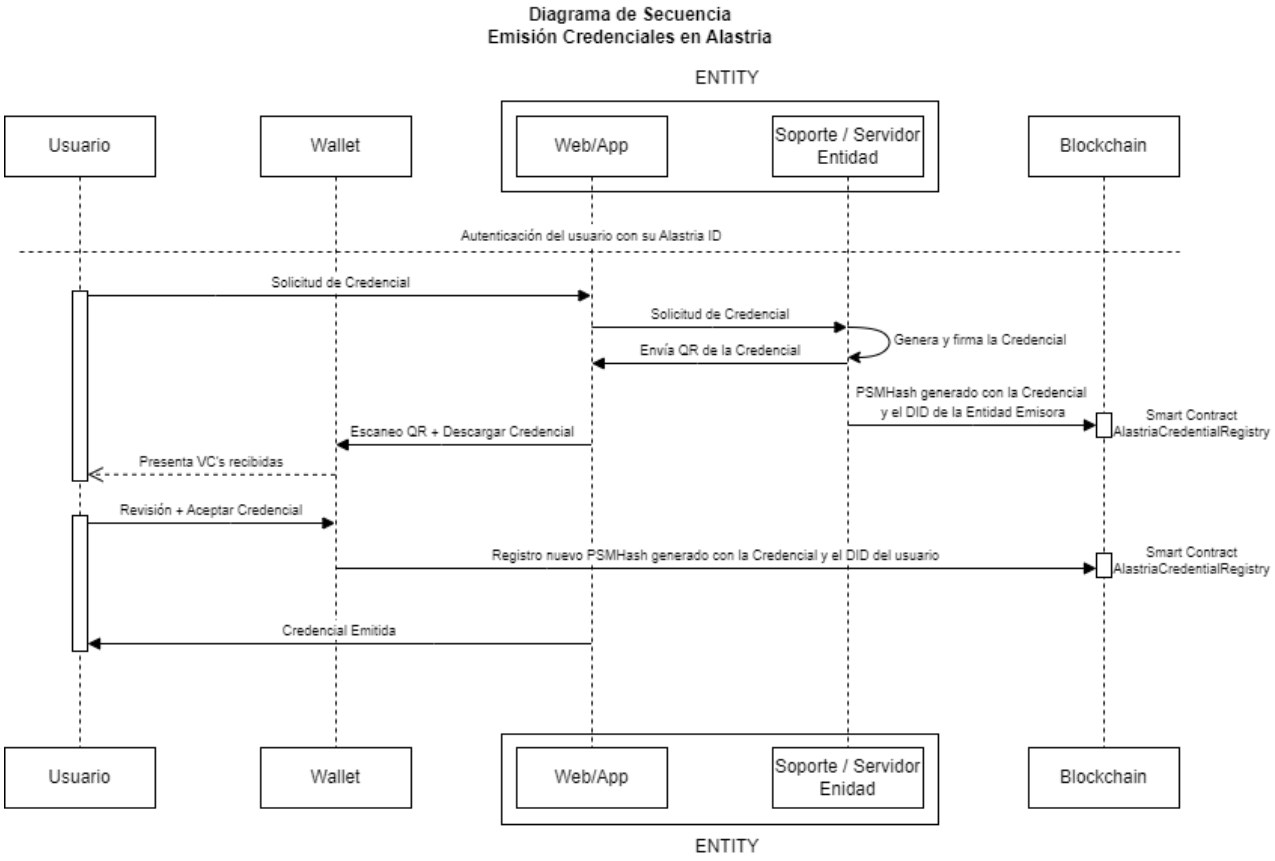


Ilustración 32 Diagrama de Secuencia Emisión de una Credencial en Alastria

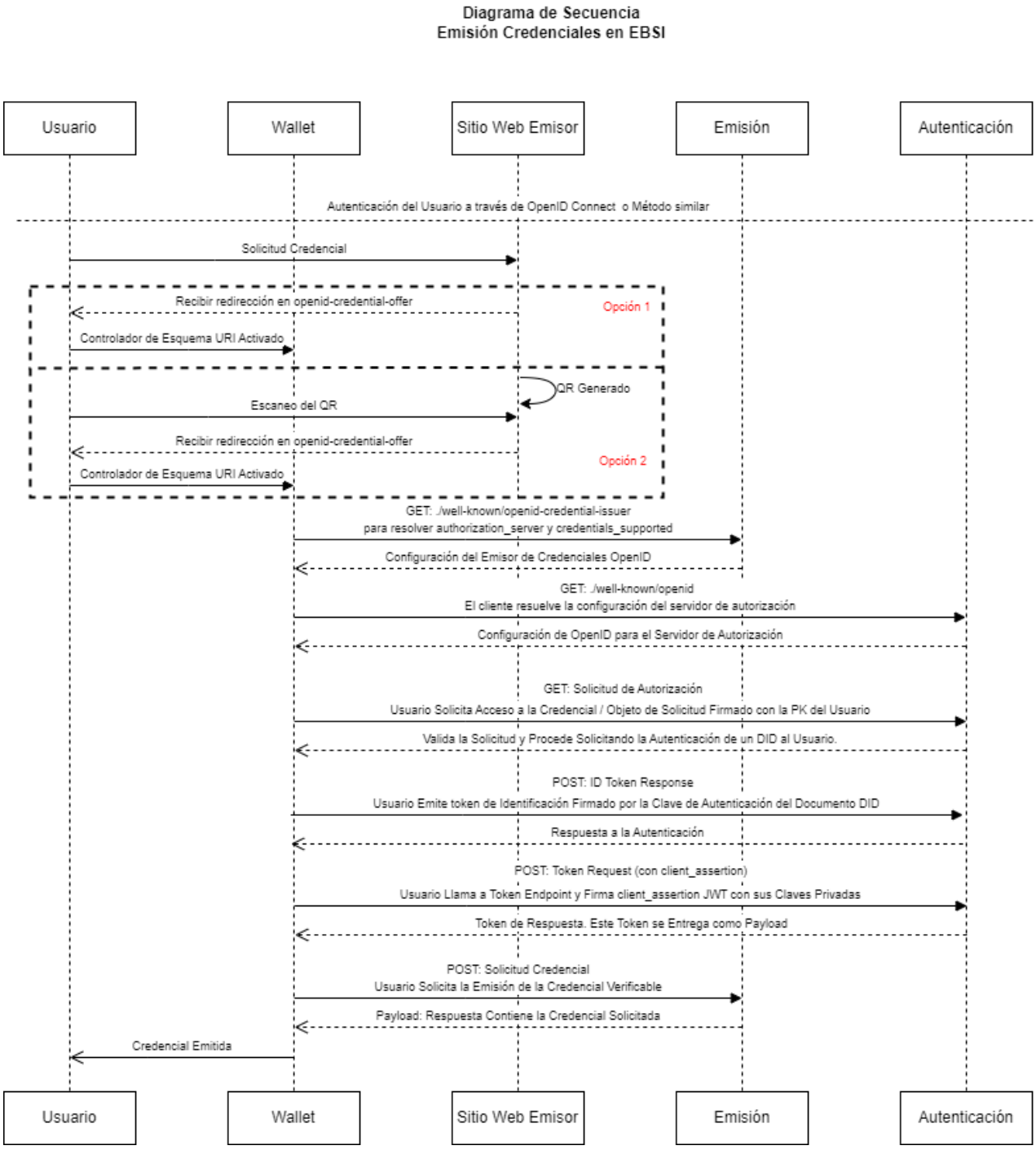


Ilustración 33 Diagrama de Secuencia Emisión de una Credencial en EBSI

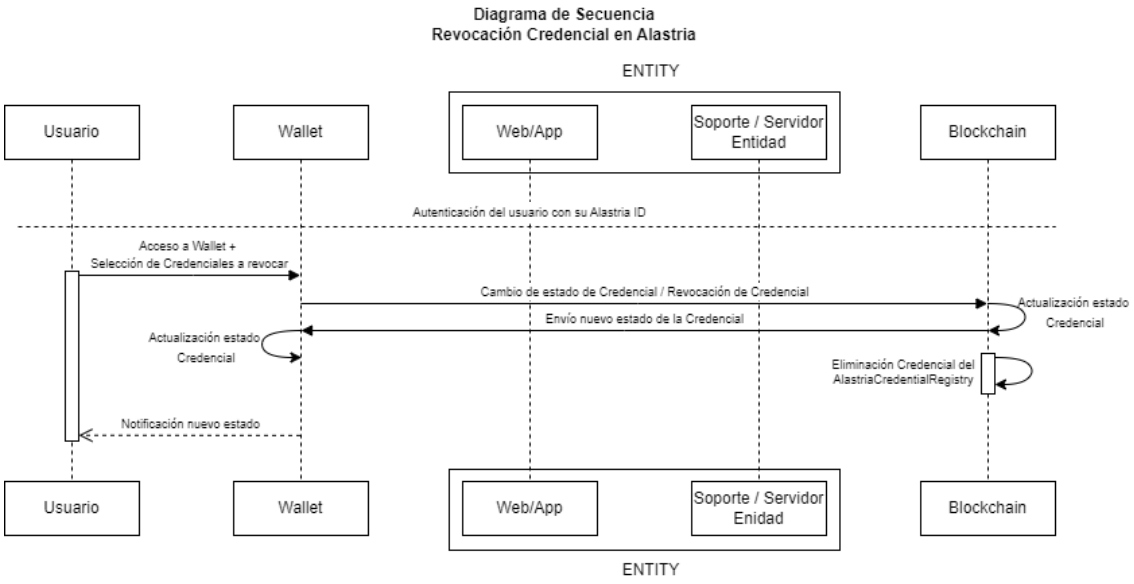


Ilustración 34 Diagrama de Secuencia Revocación de una Credencial en Alastria

4.3 Análisis de compatibilidad entre Alastria y EBSI

Se ha realizado un análisis comparativo de los diagramas de secuencia para la creación de DID en Alastria y EBSI, y para la emisión de credenciales, identificando los pasos clave del proceso y las diferencias significativas entre Alastria y EBSI.

En primer lugar, encontramos una diferencia notable ya que en EBSI los procesos se realizan mediante llamadas a la API. Esto implica que EBSI sigue un enfoque de arquitectura de servicios, esto incluye al Emisor de Credenciales, el API de Autorización, el Servicio de Registro DID, etc. Esta separación de responsabilidades en servicios independientes proporciona escalabilidad y mantenibilidad al sistema. Por otro lado, al utilizar APIs estandarizadas, EBSI facilita la interoperabilidad entre diferentes componentes y sistemas. Esto permite que aplicaciones externas, wallets u otros servicios puedan integrarse con EBSI siguiendo las especificaciones de las APIs expuestas. También las APIs pueden actuar como una capa que oculta la complejidad de los procesos internos, ya que no hace falta conocer el proceso al detalle para utilizarlo, con hacer bien el manejo de la API funcionaría todo correctamente. Por último, las APIs pueden implementar mecanismos de autenticación, autorización y control de acceso. En el caso de EBSI, nos encontramos en el diagrama de secuencia

un API de Autorización que gestiona la emisión de tokens de acceso, asegurando que solo las entidades autorizadas puedan interactuar con los servicios.

Respecto a los niveles de seguridad (LoA), en EBSI, se definen tres niveles de seguridad para la emisión de credenciales verificables: “Low, Substantial, High”. Pero con la llegada de eIDAS 2.0, se introducirá un cuarto nivel de seguridad "muy alto" para las transacciones de alto riesgo. En cuanto a Alastria, se siguen los tres niveles establecidos en eIDAS, “Low, Substantial, High”, con la diferencia de que se añade un nivel más bajo, denominado “Self”. Este nivel “Self” se utiliza en los casos en los que el propio usuario se auto emite una credencial.

En cuanto a la creación de un identificador, al inicio del proceso hay una notable diferencia, ya que en EBSI, una vez el usuario se descarga la wallet, se generan automáticamente el par de claves y se le asigna un DID, sin necesidad de interactuar con ningún sitio web para proporcionarle dicho identificador, en cambio en Alastria es necesario solicitar una autenticación al sitio web, el cuál devuelve un Alastria Token que permite al usuario continuar con el proceso de creación de un AlastriaID.

En cuanto a la gestión de claves, en Alastria, se utiliza un esquema de claves más simple, con un solo par de claves criptográficas por identidad. Este par de claves se genera y se almacena en la wallet del usuario, y se utiliza tanto para firmar transacciones como para firmar credenciales y presentaciones verificables. Respecto a EBSI, se utiliza un esquema de gestión de claves más avanzado y robusto. Por un lado se generan dos pares de claves, el primer par de claves con el algoritmo ES256K (que se utilizará para escribir datos en la blockchain) y el segundo par de claves con el algoritmo ES256 (que se utilizará para firmar credenciales y presentaciones verificables). Por otro lado, además de generar dos pares de claves, EBSI también implementa un ciclo de vida de gestión de claves. Esto permite la rotación periódica de las claves de firma de credenciales, lo que aumenta la seguridad y la privacidad a largo plazo. Las

claves antiguas se mantienen en el documento DID para permitir la verificación de credenciales emitidas previamente.

En Alastria podemos observar que el proceso entero pende de un Alastria Token (token que permite identificar a entidades o usuarios que no poseen un DID o son desconocidos en ese momento). Por un lado, al iniciar sesión por primera vez en el sitio web de la entidad, se le asigna un AT firmado por la entidad al usuario, posteriormente gracias a este token se procede a verificar la identidad de la entidad emisora, después se procede a verificar todos los campos de este AT para corroborar que todo está correcto, y finalmente, se crea el Alastria Identity Creation, artefacto que contiene el AT, y que se utilizará para los procesos finales de creación del AlastriaID. En EBSI esto mismo ocurre con el DID inicial generado una vez el usuario se descarga la wallet, puesto que una vez adquirido el DID, la wallet firma la parte inicial del Documento DID, y más tarde se procede con el proceso de añadir método de verificación y relaciones de verificación al documento DID, para obtener finalmente el documento DID final correspondiente al usuario.

Finalmente, en Alastria nos encontramos con el AlastriaID creado, el cual nos va a permitir autentificarnos en los sitios web de los emisores y en la propia wallet. En cuanto a EBSI, finalmente se habrá generado el DID correctamente. En EBSI se utilizan métodos de autenticación como puede ser SIOPv2, pudiendo utilizar otros métodos ya que no solo se limita a este.

En cuanto al proceso de emisión de credenciales, ambos procesos inician de igual forma, el usuario se autentica. Después procede a acceder al sitio web del emisor y solicita la credencial deseada. En este punto, en ambos procesos, se genera un QR con la credencial para que el usuario lo escanee con la wallet, y aquí llega la primera diferencia, EBSI en este punto también ofrece la opción de iniciar la interacción a través de una redirección, siempre y cuando el usuario acceda al sitio web del emisor desde el mismo dispositivo donde tiene instalada la wallet.

Una vez escaneado el QR, en el caso de Alastria, se le muestra al usuario una presentación de la VC para que la revise y la acepte, todo esto después de haber generado un PSMHash con la credencial y el DID de la entidad emisora, para

guardarlo en la blockchain y así certificar que la credencial ha sido emitida y poder controlar su estado de validez. Una vez el usuario la ha aceptado, se genera un nuevo PSMHash, esta vez con el DID del usuario que será el último en ser registrado en la blockchain. Finalmente, se le enviaría la credencial emitida al usuario.

En el caso de EBSI, una vez escaneado el QR, o redirigido, comienza un complejo proceso entre la wallet y los servicios de autenticación. Primero, la lógica interna de la wallet envía una solicitud de autorización firmada al Servidor de Autorización para la credencial requerida. Después de algunos redireccionamientos, la wallet demuestra el control sobre su identidad firmando un token de identificación con la clave de autenticación del documento DID. El Servidor de Autorización valida esto y responde con un código de autorización. Finalmente, el cliente (wallet) firma y envía una solicitud de token de acceso, obteniendo dicho token y un nonce de desafío (c_nonce) del Servidor de Autorización. Con el token de acceso válido, el cliente (wallet) ahora puede solicitar la emisión de la credencial al Emisor de Credenciales. Este responde con un Payload que contiene la credencial solicitada, la cual recibe la wallet y, finalmente, el usuario adquiere la credencial emitida correctamente.

5 Prueba de concepto

Para aterrizar los conceptos de identidad digital estudiados se ha realizado una pequeña prueba de concepto, cabe aclarar que ha habido muy poco tiempo para realizar esta parte del TFG, ya que este principalmente era un trabajo de investigación.

La prueba de concepto consiste en una práctica de Identidad Digital donde se utilizan los modelos ERC-725 y ERC-735 de Ethereum para reforzar los conceptos de identidad digital en la blockchain. Estos modelos permiten la gestión de identidades descentralizadas y la verificación de credenciales de manera segura y eficiente. En esta demo, se programarán una serie de funciones en el index.html para hacer las correspondientes llamadas a las funciones públicas de los Smart Contracts proporcionados. Los resultados de estas llamadas se visualizarán a través del navegador.

5.1 Objetivos

- Demostrar la funcionalidad de los contratos ERC-725 y ERC-735: Verificar que se pueden emitir y gestionar identidades digitales y sus credenciales.
- Validar la interacción entre los distintos actores (Alumno, Universidad, Empresa): Asegurar que cada entidad puede desempeñar su rol dentro del sistema de identidad digital.
- Evaluar la integración y la visualización de resultados a través de un navegador web: Comprobar que las interacciones con los contratos se reflejan correctamente en la interfaz web.

5.2 Herramientas utilizadas

Las herramientas utilizadas son:

- REMIX IDE

REMIX IDE es un entorno de desarrollo integrado accesible vía navegador que permite escribir, compilar y desplegar Smart Contracts en la blockchain. En esta práctica, se utiliza para editar, compilar y desplegar los contratos ClaimHolder.sol y ClaimVerifier.sol.

- Node.js y npm

Node.js es un entorno de ejecución para JavaScript, mientras que npm es el gestor de paquetes de Node.js. Ambos son necesarios para instalar remixd y otras dependencias del proyecto.

- remixd

remixd es una herramienta que permite conectar REMIX IDE con el sistema de archivos local. Esto facilita la edición de archivos locales directamente desde el entorno de REMIX IDE.

- Ganache

Ganache es una herramienta que permite crear una red blockchain local para pruebas. Proporciona cuentas preconfiguradas con ETH ficticio, facilitando la interacción con los contratos inteligentes sin costo.

- Python3

Python3 se utiliza para iniciar un servidor HTTP simple, necesario para servir la página web (index.html) localmente y permitir la interacción con los Smart Contracts a través del navegador.

- Visual Studio Code

Visual Studio Code se utiliza para editar los archivos de código, como index.html, para ajustar las URL y puertos de Ganache y para completar las funciones Web3.

5.3 Primeros pasos

Para realizar la prueba de concepto de Identidad Digital en Blockchain, primero se debe configurar el entorno clonando el repositorio pertinente ("git clone https://github.com/JuanLuisGozaloFdez/BlockchainLab2-identidad-2"), inicializando npm ("npm init") e instalando remixd ("npm install -g @remix-project/remixd"). A continuación, se inicia Ganache, anotando la dirección, puerto y cuentas asignadas ("./ganache-*.AppImage").

Luego, se conecta REMIX IDE con remixd ejecutando "remixd -s directorio-del-código/BlockchainLab2-identidad-2 --remix-ide http://remix.ethereum.org" y verificando que los archivos locales se muestran correctamente en REMIX IDE.

Posteriormente, se editan las URL y puerto de Ganache en index.html, se compilan y despliegan los contratos ClaimHolder.sol y ClaimVerifier.sol, asignando las cuentas a los actores correspondientes y copiando las direcciones de los contratos en index.html. Seguidamente, se completan las funciones Web3 para la emisión, aceptación y verificación de credenciales en index.html. Finalmente, se lanza la web iniciando el servidor HTTP ("python3 -m http.server") y accediendo a la página web a través del navegador en https://localhost:8000.

5.4 Diseño de la interfaz

El objetivo ha sido crear una interfaz de usuario que facilite la interacción con los contratos inteligentes de Ethereum que gestionan la identidad digital. Esta interfaz proporciona una experiencia intuitiva para los usuarios finales, permitiéndoles realizar acciones como agregar nuevas credenciales, aprobar solicitudes de credenciales y verificar la validez de las mismas. Para lograr esto, se han utilizado tecnologías como HTML, CSS y JavaScript, junto con la biblioteca web3.js, que permite la comunicación con la red Ethereum desde el navegador.

Gracias al uso de CSS hemos conseguido mejorar la estética de nuestra página web, haciéndola más agradable para el usuario e intuitiva.

```
<style>
    body {
        font-family: Arial, sans-serif;
        background-color: #f4f4f9;
        margin: 0;
        padding: 0;
    }
    .header {
        position: fixed;
        top: 0;
        left: 0;
        width: 100%;
        background-color: #007bff;
        color: white;
        padding: 10px;
        text-align: left;
        font-size: 14px;
        z-index: 1000;
    }
    .container {
        max-width: 800px;
        margin: 50px auto;
        padding: 20px;
        background-color: white;
        box-shadow: 0px 0px 10px rgba(0, 0, 0, 0.1);
        border-radius: 8px;
    }
```

```css
h1 {
    text-align: center;
    color: #333;
}
form {
    margin-top: 20px;
}
table {
    width: 100%;
    border-collapse: collapse;
    margin-top: 20px;
}
td {
    padding: 10px;
    vertical-align: top;
}
label {
    display: block;
    margin-bottom: 5px;
    color: #555;
}
input[type="text"] {
    width: calc(650px);
    padding: 10px;
    border: 1px solid #ddd;
    border-radius: 4px;
    display: inline-block;
    vertical-align: middle;
}
input[type="button"] {
    width: 200px;
    background-color: #007bff;
    color: white;
    padding: 10px;
    border: none;
    border-radius: 4px;
    cursor: pointer;
    display: inline-block;
    vertical-align: middle;
}
```

```
    input::placeholder {
        font-style: italic;
        color: rgba(0, 0, 0, 0.5);
    }
    #console {
        margin-top: 20px;
        padding: 20px;
        background-color: #f9f9f9;
        border: 1px solid #ddd;
        border-radius: 4px;
        min-height: 50px;
        line-height: 1.8;
        overflow: auto;
        white-space: pre-wrap;
    }
    #console2 {
        margin-top: 20px;
        padding: 20px;
        background-color: #f9f9f9;
        border: 1px solid #ddd;
        border-radius: 4px;
        min-height: 50px;
        line-height: 2;
    }
    .console-title {
        font-weight: bold;
        margin-bottom: 10px;
    }
    #mensaje {
        margin-top: 10px;
        color: #28a745;
    }
</style>
```

Estas tres imágenes contienen la implementación utilizada para mejorar la estética de nuestra página web a través de CSS.

Finalmente, el aspecto visual de la página web sería el siguiente:

Identidad Digital Demo

Dirección del contrato Alumno:

Ej:0x123D3e68a20A72CfCB95a9556b4F063443abF6aa

Dirección del contrato Universidad:

Ej:0x12B25835Dde7E349b8291Fd1426217D1a2dbAb04

Dirección del contrato Empresa:

Ej:0xdd56440F7a5F363664BB2CE30d1f563191624388

Almacenar Direcciones

Par de Claves

Clave privada:

Clave publica:

Universidad

Clave para firma de credenciales:

getKey

Añadir clave a la universidad para firmar credenciales:

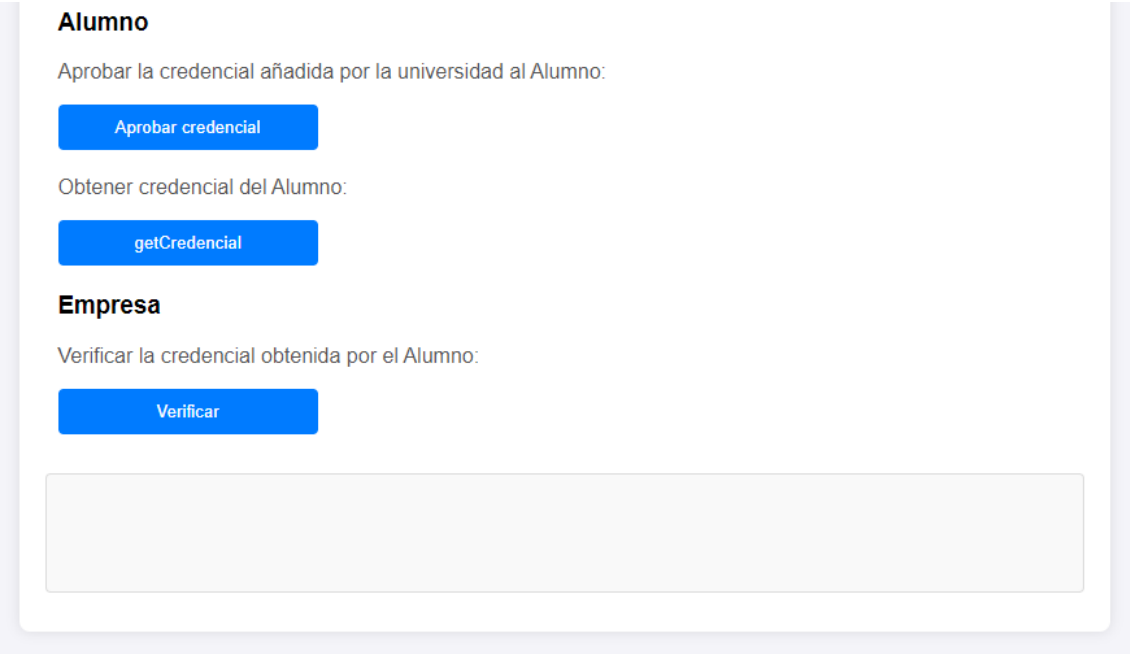
addKey_Uni

Añadir credencial y solicitar credencial de la Universidad al Alumno:

Posee certificado Experto Universitario en Desarrollo de Aplicaciones Blockchain

Añadir

Alumno



5.5 Desarrollo de la aplicación web

A continuación se explicarán las funciones realizadas en JavaScript para conseguir todas las funcionalidades necesarias.

start()

Con esta función asincrónica, se inicia la interacción con la red Ethereum. Primeramente, se obtienen todas las cuentas disponibles en la red utilizando web3.eth.getAccounts(). A través de la llamada initializeInstance() inicializamos las instancias de los contratos. Luego, se almacenan las cuentas del alumno, la universidad y la empresa en variables correspondientes. Finalmente, se crea un par de claves pública y privada para la firma de credenciales y claves.

```
async function start() {

    // Gett all the accounts
    const accounts = await web3.eth.getAccounts();

    //Cuentas
    cuentaAlumno = accounts[0];
    cuentaUni = accounts[1];
    cuentaEmpresa = accounts[2];

    console.log("Direccion de cuenta del Alumno:", cuentaAlumno);
    console.log("Direccion de cuenta de la Universidad:", cuentaUni);
    console.log("Direccion de cuenta de la Empresa:", cuentaEmpresa);

    initializeInstance();

    // Create public and private signer for claims and keys
    prvSigner = web3.eth.accounts.create().privateKey;
    pubSigner = web3.eth.accounts.privateKeyToAccount(prvSigner).address;
    console.log("Clave privada pvrSigner: " + prvSigner);
    console.log("Clave publica pubSigner: " + pubSigner);

}

start();
```

almacenarDirecciones()

Esta función asincrónica se utiliza para almacenar las direcciones de los contratos inteligentes. Obtiene las direcciones de los contratos del HTML, las valida y las almacena. Luego, inicializa las instancias de los contratos inteligentes.

```
function almacenarDirecciones () {
    contrato_alumno = document.getElementById('contrato_alumno').value;
    contrato_uni = document.getElementById('contrato_uni').value;
    contrato_empresa = document.getElementById('contrato_empresa').value;

    // Validar direcciones
    if (!web3.utils.isAddress(contrato_alumno) || !web3.utils.isAddress(contrato_uni) || !web3.utils.isA
        alert("Una o más direcciones no son válidas. Por favor, verifica las direcciones ingresadas.");
        return;
    }

    console.log("Direccion de contrato del Alumno:", contrato_alumno);
    console.log("Direccion de contrato de la Universidad:", contrato_uni);
    console.log("Direccion de contrato de la Empresa:", contrato_empresa);

    initializeInstance();

    updateConsole2(prvSigner, pubSigner);

    document.getElementById('console2').innerHTML += `
        Direcciones de contrato:<br>
        Direcci&oacute;n contrato Alumno: ${contrato_alumno}<br>
        Direcci&oacute;n contrato Universidad: ${contrato_uni}<br>
        Direcci&oacute;n contrato Empresa: ${contrato_empresa}`;
};
```

initializeInstance()

Esta función asincrónica inicializa las instancias de los contratos inteligentes utilizando el ABI (Interfaz de Contrato Inteligente) proporcionado y las direcciones de los contratos almacenados previamente.

```
function initializeInstance() {
    instanciaAlumno = new web3.eth.Contract(ABI_CH,contrato_alumno);
    instanciaUni = new web3.eth.Contract(ABI_CH, contrato_uni);
    instanciaEmpresa = new web3.eth.Contract(ABI_CV, contrato_empresa);
    console.log("Instancia Alumno:", instanciaAlumno);
    console.log("Instancia Universidad:", instanciaUni);
    console.log("Instancia Empresa:", instanciaEmpresa);
}
```

getKey()

Esta función obtiene una clave específica de un contrato de una universidad. Utiliza el método getKey del contrato del alumno para obtener la clave correspondiente.

```
//Clave para alumno
async function getKey() {//UNI
    document.getElementById('mensaje').innerHTML = "";
    var key = web3.utils.keccak256(pubSigner);
    let result = [];

    result = await instanciaUni.methods.getKey(key).call();

    if(result.key == "0x0000000000000000000000000000000000000000000000000000000000000000"){
        console.log(result);
        document.getElementById('console').innerHTML += "<br>No hay claves por el momento con el pro
    }else{
        console.log(result);
        document.getElementById('console').innerHTML += "<br>La clave obtenida es: " + result.key;
    }
}
```

addKey()

Esta función añade una clave al contrato de la universidad para firmar credenciales. Utiliza el método addKey del contrato de la universidad para agregar la clave con el propósito y tipo especificados. La transacción se envía desde la cuenta de la universidad.

```
//añadir clave a la universidad para firmar alegaciones
async function addKey(){//UNI
    document.getElementById('mensaje').innerHTML = "";
    var key=web3.utils.keccak256(pubSigner);
    console.log("Key keccack: ",key);
    var fgas=await instanciaUni.methods.addKey(key,3,1).estimateGas({from: cuentaUni});
    var result=await instanciaUni.methods.addKey(key,3,1).send({from: cuentaUni, gas:fgas});

    if (result.events.KeyAdded) {
        console.log("Evento keyadded clave añadida");
        console.log("Key:",result.events.KeyAdded.returnValues.key);
        console.log("Pourpose:",result.events.KeyAdded.returnValues.purpose);
        console.log("Type:",result.events.KeyAdded.returnValues.keyType);
        console.log("BlockNumber:",result.blockNumber);
        document.getElementById('console').innerHTML += "<br><br>Transaccion enviada";
        document.getElementById('console').innerHTML += "<br>La clave " + result.events.KeyAdded.returnValues.key +
        document.getElementById('mensaje').innerHTML = "La clave para firmar credenciales se ha a&ntilde;adido corre
    } else {
        console.log('Evento keyadded no lanzado');
        document.getElementById('console').innerHTML += "<br><br>Error en la transaccion: " + error.message;
    }
}
```

addClaimUniAlumno(credencial)

Esta función se encarga de añadir una credencial específica (claim) al contrato de identidad de un alumno desde la universidad. Esta función permite a la universidad registrar una credencial en la identidad del alumno de manera segura y verificable.

```
//Añadir alegacion/CREDENCIAL desde la universidad en el contrato de identidad del Alumno (addClaim)
async function addClaimUniAlumno(credencial) {
    //Obtener Abi de instanciaAlumno.methods.addClaim()
    document.getElementById('mensaje').innerHTML = "";
    var claimType = 3; //TIPO DE CREDENCIAL
    var claimSchema = 1;
    var issuer = instanciaUni._address;
    var data = web3.utils.asciiToHex(credencial);
    var hashed = web3.utils.soliditySha3(issuer, claimType, data); //Hasheamos la direccion del issuer + claimType + data
    var signed = await web3.eth.accounts.sign(hashed, prvSigner); //lo firmamos con la clave privada
    var signature = signed.signature;
    console.log("Parametro signature:",signature);

    var gasLimitt = await instanciaAlumno.methods.addClaim(claimType,claimSchema,issuer,signature,data,"https://ethereum.org/es/").estimateGas({ from: cuentaAlumno });
    var claimRes = await instanciaAlumno.methods.addClaim(claimType,claimSchema,issuer,signature,data,"https://ethereum.org/es/").send({ from: cuentaAlumno, gas: gasLimitt });
    if (claimRes.events.ClaimAdded) {
        document.getElementById('console').innerHTML += "<br><br>Credencial a&ntilde;adida";
    } else {
        console.error("Error addClaim:", error);
    }
    console.log(claimRes);
    //Obtener Abi de instanciaAlumno.methods.addClaim()
    var addClaimAbi = await instanciaAlumno.methods.addClaim(claimType,claimSchema,issuer,signature,data,"https://ethereum.org/es/").encodeABI();
    //Usar la funcion instanciaAlumno.methods.execute()
    var gasLimit = await instanciaAlumno.methods.execute(instanciaAlumno._address, 0, addClaimAbi).estimateGas({ from: cuentaUni });
    var response = await instanciaAlumno.methods.execute(instanciaAlumno._address,0,addClaimAbi).send({ from: cuentaUni, gas: gasLimit });

    if (response.events.ExecutionRequested) {
        console.log("Evento ExecutionRequested: credencial requerida");
        console.log("Execution ID:", response.events.ExecutionRequested.returnValues.executionId);
        document.getElementById('console').innerHTML += "<br><br>ID de la credencial: " + response.events.ExecutionRequested.returnValues.executionId;
    } else {
        console.log("Evento ExecutionRequested: no lanzado");
    }

    if (response.events.Approved) {
        console.log("Evento Approved: credencial aprobada");
    } else {
        console.log("Evento Approved: no lanzado");
    }

    if (response.events.Executed) {
        console.log("Evento Executed: credencial ejecutada");
    } else {
        console.log("Evento Executed: no lanzado");
    }

    id = response.events.ExecutionRequested.returnValues.executionId;

    console.log(response);
}
```

approveUniAlumno()

Esta función tiene como objetivo aprobar una credencial que ha sido añadida por la universidad para un alumno. En este contexto, aunque la universidad haya expedido la credencial, es necesario que el alumno la apruebe para que esta sea considerada válida.

```
//Aprobar la alegacion/CREDENCIAL añadida por la universidad al Alumno (approve), ya que la Universidad la ha
async function approveUniAlumno() {//ALUMNO
    document.getElementById('mensaje').innerHTML = "";
    //Usar la funcion instanciaAlumno.methods.approve()
    var approval = await instanciaAlumno.methods.approve(id,true).send({ from: cuentaAlumno, gas: gasLimit });
    if (approval.events.Approved) {
        console.log("Evento Approved: credencial aprobada");
        console.log("La credencial con ID", id, "ha sido aprobada exitosamente");
        document.getElementById('console').innerHTML += "<br><br>La credencial ha sido aprobada exitosamente";
        document.getElementById('mensaje').innerHTML = "Credencial aprobada correctamente";
    } else {
        console.log("Evento Approved: no lanzado");
    }

    if (approval.events.ClaimAdded) {
        console.log("Evento ClaimAdded: credencial a&ntilde;adida");
        document.getElementById('console').innerHTML = document.getElementById('console').innerHTML +
        "<br>"+
        "ClaimAdded <br>Claim Type = " + approval.events.ClaimAdded.returnValues.claimType +
        ", Issuer = " + approval.events.ClaimAdded.returnValues.issuer;
    } else {
        console.log("Evento ClaimAdded: no lanzado");
    }

    if (approval.events.Executed) {
        console.log("Evento Executed: credencial ejecutada");
        document.getElementById('console').innerHTML = document.getElementById('console').innerHTML +
        "<br>"+
        "Executed <br>Execution Id = " + approval.events.Executed.returnValues.executionId;
    } else {
        console.log("Evento Executed: no lanzado");
    }

    console.log(approval);
}
```

getClaim()

La función getClaim se encarga de obtener y mostrar una credencial específica del contrato del alumno. Utilizando el método getClaim del contrato del alumno (instanciaAlumno), se realiza una llamada para obtener los detalles de la credencial correspondiente al claimId generado.

```
async function getClaim() {
    var claimId = web3.utils.soliditySha3(instanciaUni._address, 3);
    var claim = await instanciaAlumno.methods.getClaim(claimId).call();

    document.getElementById('console').innerHTML = document.getElementById('console').innerHTML +
        "<br><br>CREDENCIAL del Alumno:<br>"+
        "{Claim Type = " + claim.claimType +
        ", Issuer = " + claim.issuer +
        ", <br>Data = " + claim.data +
        ", <br>Signature = " + claim.signature + "}";

    console.log(claim);
}
```

verifierUniAlumno()

Esta función está diseñada para que una empresa verifique una credencial hecha por la universidad sobre un alumno. Esta verificación confirma que el alumno posee la credencial, que es válida y ha sido aprobada.

```
//Verificar la credencial por parte de la empresa (checkClaim) de que el alumno tiene ese claim/CREDENCIAL y es válido y está aprob
async function verifierUniAlumno() {//EMPRESA
    document.getElementById('mensaje').innerHTML = "";
    //Usar la funcion  instanciaEmpresa.methods.checkClaim()
    var fgas = await instanciaEmpresa.methods.checkClaim(instanciaAlumno._address,3).estimateGas({ from: cuentaEmpresa });
    var resultado = await instanciaEmpresa.methods.checkClaim(instanciaAlumno._address,3).send({ from: cuentaEmpresa, gas: fgas });
    if (resultado.events.ClaimValid) {
        console.log("Verificacion por parte de la empresa exitosa");
        document.getElementById('console').innerHTML = "<br><br>La empresa ha verificado exitosamente que el alumno tiene la creden
        document.getElementById('console').innerHTML = document.getElementById('console').innerHTML +
        "<br>"+
        "{Block Number = " + resultado.blockNumber +
        ", ClaimValid, Identity = " + resultado.events.ClaimValid.returnValues._identity +
        ", Claim Type = " + resultado.events.ClaimValid.returnValues.claimType + "}";
    }
    else if (resultado.events.ClaimInvalid) {
        console.log("Evento ClaimInvalid: credencial no validada");
        console.error("Error al verificar la credencial");
        document.getElementById('console').innerHTML += "<br><br>Error al verificar la credencial: ";
    } else {
        console.log("Evento ClaimValid: no lanzado");
        console.log("Evento ClaimInvalid: no lanzado");
    }
    console.log(resultado);
}
```

5.6 Conclusiones de la implementación

En primer lugar esta implementación me ha servido para acercarme un poco más a lo que es la realidad de la identidad digital y blockchain. He podido desplegar por primera vez Smart Contracts por mí mismo, he aprendido a diferenciar lo que es un contrato y una instancia entre otros muchos conceptos. Otro tópico que a veces se dificulta a la hora de interactuar con ciertas funciones es la firma con las claves públicas y privadas. En esto encontré gran dificultad ya que no tenía mucho conocimiento sobre ello. Después de muchas horas debuggeando el código, he podido asentar mejor los conocimiento sobre este tema.

El objetivo de esta implementación ha sido trasladar conocimientos teóricos vistos en la investigación sobre la creación de credenciales, emisión de credenciales, aprobación de credenciales, etc. De esta manera hemos conseguido implementar una app capaz de emitir credenciales (a través del uso de addClaim()), aceptar credenciales (a través del uso de approveClaim()) y verificar una presentación realizada (a través del uso de checkClaim()).

6 Resultados y conclusiones

Resumen de resultados obtenidos en el TFG. Y conclusiones personales del estudiante sobre el trabajo realizado.

El trabajo realizado en este TFG tiene un gran valor en cuanto al contenido de investigación, ya que la mayor parte del trabajo ha sido orientada hacia un estudio y análisis de los principales modelos de identidad digital. Como bien se ve, el trabajo de investigación ha sido exhaustivo, ya que se ha buscado alrededor de todo el mundo modelos de identidad digital, proyectos de identidad digital, estándares, proyectos de identidad autogestionada, etc. Se ha finalizado este proyecto de investigación con un análisis comparativo entre el modelo español Alastria y el modelo europeo EBSI.

En cuanto a EBSI cabe destacar que la información disponible en el repositorio oficial está muy enrevesada, encuentro falta de contenido y de diagramas UML, los cuales considero esenciales y son un puto clave en la ingeniería de software. Debido a esto, el análisis de EBSI, centrado en el funcionamiento de la creación de un id y de la emisión de credenciales, se ha visto dificultado, repercutiendo en el posterior análisis comparativo entre Alastria ID y EBSI. En cuanto al proceso de revocación de credenciales, si bien Alastria muestra un proceso de cómo se realiza y proporciona la información necesaria para llevar a cabo esta revocación, en el caso de EBSI no es igual. EBSI proporciona cual sería la forma en la que funcionase este proceso, pero no ofrece al cliente las API's necesarias para probar que este servicio este vigente y las empresas lo estén utilizando, por lo que no podemos concluir con exactitud que actualmente esté en funcionamiento.

Finalmente, considero en base al estudio realizado, que la compatibilidad entre Alastria y EBSI es baja, debido a la diferencia de procesos y funcionamientos.

7 Análisis de Impacto

En este capítulo se realizará un análisis del impacto potencial de los resultados obtenidos durante la realización del TFG en diferentes contextos.

En el ámbito personal, este trabajo me ha aportado un gran valor y un nuevo punto de vista sobre la importancia de la identidad digital. He podido ver los beneficios que el modelo self-sovereign identity puede proporcionar a la sociedad actual. Me he podido sumergir en el punto de vista internacional sobre este tópico, pudiendo estudiar cómo está evolucionando en otros países y descubrir incipientes proyectos con un gran potencial. También me ha ayudado a agilizar mi lectura en inglés, debido a la cantidad de documentación en inglés que he necesitado leer para la redacción del trabajo.

En el ámbito empresarial, este trabajo supone un gran beneficio para aquellas empresas que necesiten información sobre cómo está evolucionando la identidad digital en otros países, así como conocer si han surgido nuevos proyectos y estándares. Además, gracias a este trabajo serán más conscientes de la importancia del modelo de identidad autogestionado. Finalmente, supondrá un gran valor para aquellas empresas que están buscando como compatibilizar los modelos de Alastria y EBSI, ya que se aporta un punto de vista sobre este tópico entrando en el análisis de los princípiales procesos que se llevan a cabo, creación de un identificador, emisión de credenciales y revocación de credenciales.

En el ámbito social y cultural, este trabajo permitirá dar a conocer la importancia de la evolución de la identidad digital, y cómo el modelo de identidad autogestionada puede dar solución a una gran cantidad de problemáticas. Además, dado que, al emplear una tecnología relativamente nueva (blockchain), es necesario depositar confianza en esta, y la mejor forma es desde el conocimiento del funcionamiento, por lo que este trabajo aportará la información necesaria para comprender cómo funciona la tecnología blockchain y por qué confiar en esta tecnología.

8 Bibliografía

Alastria actúa como hub de conexión. (n.d.). Retrieved April 11, 2024, from https://alastria.io/que-hacemos/#ecosistema

Alastria Digital Identity. (2019).

Alastria ID flows · alastria/alastria-identity . (n.d.). Retrieved April 17, 2024, from https://github.com/alastria/alastria-identity/wiki/Alastria-ID-flows

Alexander Preukschat. (2017). *Blockchain La revolución industrial de internet*.

Anthopoulos, L. (2021). *Guidelines on energy efficient blockchain systems*.

Blockchain: conoce la tecnología - CPQD. (n.d.). Retrieved March 21, 2024, from https://www.cpqd.com.br/es/blockchain/

Borak, M. (2023). *Japan trying to get it right with national digital ID, public losing faith | Biometric Update*. https://www.biometricupdate.com/202308/japan-trying-to-get-it-right-with-national-digital-id-public-losing-faith

Brasil lanza identificación digital basada en blockchain. (2023). https://es.cointelegraph.com/news/brazil-rolls-out-blockchain-based-digital-id

Carteira de Identidade Nacional chega a 24 unidades da federação. (2024). https://www.serpro.gov.br/menu/noticias/noticias-2024/carteira-identidade-nacional-24-unidades-federacao

Chomczyk, A. (2020). *Regulacion-de-blockchain-e-identidad-digital-en-America-Latina*.

ConnectID - Australian Payments Plus. (n.d.). Retrieved April 9, 2024, from https://www.auspayplus.com.au/brands/connectid

ConnectID - Digital identity verification. (n.d.). Retrieved April 9, 2024, from https://connectid.com.au/

Dalion | Inetum. (n.d.). Retrieved April 16, 2024, from https://www.inetum.com/es/spain/noticias/dalion-la-solucion-de-identidad-digital-autogestionada-premio-en-los-blockchain

Dalion - Alastria. (n.d.). Retrieved April 16, 2024, from https://alastria.io/dalion/

Digital Identity | myGov. (n.d.). Retrieved April 8, 2024, from https://my.gov.au/en/about/help/digital-identity

Domingo, I. A. (2020). *SSI eIDAS Legal Report*. http://www.europa.eu

EBSI high-level presentation. (2024).

eIDAS 2: Fechas, novedades, EUDI y la nueva wallet. (n.d.). Retrieved April 15, 2024, from https://www.tecalis.com/es/blog/eidas2-eidas-2-reglamento-eudi-20-europa-ue-wallet

eIDAS2 EDIW. (2024).

Emitir Documentos Digitales - Xertify. (n.d.). Retrieved April 4, 2024, from https://xertify.co/

Gloria, P. (2023). *EMPOWERING FINANCIAL INCLUSION IN MEXICO THROUGH SSI SELF-SOVEREIGN IDENTITY*. https://www.gphlegal.mx/2023/10/18/empowering-financial-inclusion-in-mexico-through-ssi-self-sovereign-identity-2/

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017a). *Digital identity guidelines: revision 3*. https://doi.org/10.6028/NIST.SP.800-63-3

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017b). *Digital identity guidelines: revision 3*. https://doi.org/10.6028/NIST.SP.800-63-3

Home | Digital Identity. (n.d.). Retrieved April 8, 2024, from https://www.digitalidentity.gov.au/

Home - EBSI -. (n.d.). Retrieved April 15, 2024, from https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

How India is using digital technology to project power. (2023). https://www.economist.com/asia/2023/06/04/how-india-is-using-digital-technology-to-project-power

iD: monedero de credenciales digitales basado en blockchain -CPQD. (n.d.). Retrieved March 21, 2024, from https://www.cpqd.com.br/es/solucoes/id/

India Stack. (n.d.). Retrieved April 5, 2024, from https://indiastack.org/

Infraestructura europea de servicios Blockchain | Configurar el futuro digital de Europa. (n.d.). Retrieved April 15, 2024, from https://digital-strategy.ec.europa.eu/es/policies/european-blockchain-services-infrastructure

Inquiry into the Digital ID Bill 2023 and the Digital ID. (2024).

Introduction to Trust Over IP. (2021).

IOME. (n.d.). Retrieved April 5, 2024, from https://iome.ai/

Kim, D., & Kokuryo, J. (2024). Establishing altruistic ethics to use technology for Social Welfare—How Japan manages Web3 and self-sovereign identity in local communities. *Electronic Markets*, *34*(1). https://doi.org/10.1007/s12525-023-00684-x

Krishnan -Founder, A. (2023). *INTERACTION STATE MACHINES & CONTEXT-AWARE BLOCKCHAIN NETWORKS*. www.moi.technology

Los 3 principales tipos de redes Blockchain - Hypernifty Academy. (2022). https://observatorioblockchain.com/hypernifty/redes-blockchain-tipos/

Luis, J., & Ugarte, R. (2018). *Tecnología de registros distribuidos (DLT): una introducción. Artículos Analíticos. Boletín Económico 4/2018*.

Macdonald, A. (2023). *Japan's digital ID system suffers new glitch as govt seeks to get ahead of failures | Biometric Update*. https://www.biometricupdate.com/202310/japans-digital-id-system-suffers-new-glitch-as-govt-seeks-to-get-ahead-of-failures

MOI - Humanize the Internet. (n.d.). Retrieved April 5, 2024, from https://moi.technology/

Nagware, K. (2023). *The Role of Blockchain based Decentralized Identity(SSI/ DID) in India's DPDP* . https://www.linkedin.com/pulse/role-blockchain-based-decentralized-identityssidid-indias-nagware/

National Blockchain Project. (n.d.). Retrieved April 5, 2024, from https://blockchain.cse.iitk.ac.in/#about

OpenID for Verifiable Credentials. (2022).

Pastor Matut, C. (2024). *La nueva identidad digital europea*.

Phillip J. Windley. (2018). *Multi-Source and Self-Sovereign Identity*. https://www.windley.com/archives/2018/09/multi-source_and_self-sovereign_identity.shtml

Ping Soon, K. (2018). *El gobierno de Singapur se convierte en "nativo digital" | Apolítico*. https://apolitical.co/solution-articles/es/nativo-digital-de-singapur

Plataforma Blockchain Alastria. (n.d.). Retrieved April 11, 2024, from https://alastria.io/que-es-alastria/

POLÍTICAS GOBIERNO Y OPERACIÓN RED ALASTRIA V1.01. (n.d.).

Portal de Gobierno Digital de Colombia. MinTIC. (n.d.). Retrieved April 2, 2024, from https://gobiernodigital.mintic.gov.co/portal/

Preukschat, A., Reed, D., Allen, C., & Vogelsteller, F. (2021a). *From eIDAS to SSI in the European Union*.

Preukschat, A., Reed, D., Allen, C., & Vogelsteller, F. (2021b). *Self-Sovereign Identity Chapter 1 Why the internet is missing an identity layer—and why SSI can finally provide one*.

Preukschat, A., Reed, D., Allen, C., & Vogelsteller, F. (2021c). *Self-Sovereign Identity Chapter 2 The basic building blocks of SSI*.

Proyecto DIDI - Argentina. (2023).

¿Qué es «Singpass»? | Crypto.com. (n.d.). Retrieved April 19, 2024, from https://help.crypto.com/es/articles/5736234-que-es-singpass

Registraduría Nacional del Estado Civil. (n.d.). Retrieved April 2, 2024, from https://www.registraduria.gov.co/-Portada-.html

Renee Yang. (2019). *Blockchain Technology Explained*. https://medium.com/swlh/a-simple-guide-to-blockchain-technology-4589971e6d03

Ruiz García, Antonio (2020). *Desarrollo de una aplicación web del modelo de identidad soberana Alastria ID*

https://oa.upm.es/71321/

Singpass. (n.d.). Retrieved April 19, 2024, from https://www.tech.gov.sg/products-and-services/singpass/

Singpass - Your Improved Digital ID. (n.d.). Retrieved April 19, 2024, from https://www.singpass.gov.sg/main/

Suárez, C. (2021). *Xertify Signature: La manera más simple de emitir documentos que deben ser firmados por varios actores* . https://www.linkedin.com/pulse/xertify-signature-la-manera-m%C3%A1s-simple-de-emitir-que-deben-su%C3%A1rez/?originalSubdomain=es

Tatiana Revoredo. (2020). *Self-Sovereign Digital Identity: The Management of Identities and the Ability to Prove Who We Are. Brasil*. https://www.legalbusinessworld.com/post/self-sovereign-digital-identity-the-management-of-identities-and-the-ability-to-prove-who-we-are

Tecnología blockchain: aplicación en Finanzas. EUDE Business School. (2018). https://www.eude.es/blog/tecnologia-blockchain-caracteristicas/

THE PUBLIC SECTOR PROFILE OF THE PAN-CANADIAN TRUST FRAMEWORK. (2021).

What is EBSI - EBSI -. (n.d.). Retrieved April 15, 2024, from https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+is+ebsi

9 Anexos

A continuación, se detallarán los pasos que se desarrollan en los diagramas de secuencia del capítulo 4.2 Diseño de diagramas de secuencia propios:

El proceso de creación de un Alastria ID

1. Un nuevo usuario accede al sitio web de una entidad emisora de credenciales. El usuario debe haberse registrado previamente para obtener un Legacy ID en dicha entidad.
2. Una vez que el usuario ha iniciado sesión en el sitio web, aparece la opción de crear un Alastria ID, a través del despliegue de un código QR en la pantalla. Este código QR contiene un Alastria Token firmado por la entidad con su clave privada.
3. El usuario escanea este código QR utilizando una aplicación wallet instalada en su teléfono (si el usuario no tiene una wallet en su teléfono, le aparecerá un código QR para descargarla ya sea en Android como iOS).
4. Tras escanear el código QR, la aplicación wallet, verifica la identidad de la entidad utilizando el DID del Alastria Token y obtiene su clave pública en el Smart Contract AlastriaPublicKeyRegistry.
5. Una vez que la identidad de la entidad ha sido verificada, la aplicación wallet verifica la validez de todos los campos del Alastria Token. Si todos los campos son válidos, el wallet crea un artefacto de tipo Alastria Identity Creation. Este artefacto contiene el Alastria Token recibido, la transacción createAlastriaTX y la clave pública del usuario, todos ellos firmados por la clave privada del usuario.
6. Una vez creado este artefacto, la entidad emisora de credenciales lo recibe (el AIC) y verifica la procedencia del token utilizando la clave pública del usuario.
7. Luego, la entidad realiza las transacciones prepareAlastriaID y createAlastriaID en el Smart Contract AlastriaIdentityManager, generando así el despliegue de un nuevo Alastria Proxy que contiene el DID del nuevo usuario, enlazándolo con el EOA (cuenta en Ethereum) del usuario.

8. Finalmente, la clave pública del usuario se registra en el AlastriaPublicKeyRegistry vinculada a su DID. Además, la entidad asocia el DID generado al Legacy ID del usuario desde su Backend.
9. Una vez terminado todo esto, el Alastria ID está creado.

El proceso de emisión de una credencial en Alastria

1. Primeramente, el usuario accede a la página web de la entidad emisora de credenciales, iniciando sesión con su correspondiente Alastria ID.
2. Una vez iniciada sesión, el usuario selecciona la credencial, la cual contiene información verificada por la entidad, que quiere que sea emitida.
3. A la par que aparece en la web un código QR con la credencial firmada, se guarda en el Smart Contract AlastriaCredentialRegistry un PSMHash generado con la credencial y el DID de la Entidad Emisora de Credenciales. Este PSMHash se utiliza para certificar que la credencial ha sido emitida y permite que la entidad controle su estado de validez.
4. El usuario escanea el código QR generado, a través de su aplicación wallet, y verifica la credencial.
5. Después de esto, la aplicación wallet muestra las credenciales solicitadas junto a un botón para que el usuario termine de confirmar la aceptación de estas credenciales. Al aceptarlas, se registra un nuevo PSMHash en el AlastriaCredentialRegistry. Este nuevo PSMHash, formado por la credencial y el DID del usuario, indica que el usuario ha aceptado estas credenciales y le permite controlar su estado.
6. Finalmente, ya estaría emitida la credencial.

El proceso de revocación de una credencial en Alastria

1. El usuario únicamente tendría que acceder a su wallet personal y seleccionar las credenciales que quiere revocar y cambia su estado.
2. De esta forma lo que ocurre es que la credencial se elimina del AlastriaCredentialRegistry o la presentación del AlastriaPresentationRegistry.

El proceso de creación de un ID en EBSI

1. El usuario se descarga la aplicación wallet.
2. Generación de pares de claves: El paso inicial en la creación de una identidad digital EBSI es la generación de un par de claves criptográficas. Este par consta de una clave pública y otra privada. La clave privada se almacena de forma segura en una cartera digital y sólo puede acceder a ella el propietario.
3. Creación del DID: Con el par de claves, se crea un Identificador Descentralizado (DID). Este DID actúa como identificador único en el ecosistema EBSI.
4. El usuario debe recibir una credencial VerifiableAuthorisationToOnboard emitida por un emisor de confianza existente con una función TAO.
5. A continuación, el usuario debe solicitar un Token de Acceso didr_invite a la API de autenticación EBSI, que responde con una Verifiable Presentation y una Presentation Submission. La respuesta se envía al punto final /token de la API de autenticación. Si el envío se realiza correctamente, la API de autenticación EBSI emite un token de acceso de corta duración compatible con OAuth 2.0 basado en la presentación verificable presentada.
6. El usuario puede registrar la parte inicial del documento DID con la clave ES256K, utilizando el método insertDidDocument.
7. La wallet recibirá la transacción Ethereum con el formato correcto para ser firmada. Una vez firmada la transacción, está lista para su envío mediante el método sendSignedTransaction, que actualiza la blockchain.
8. El usuario solicita un token de acceso con el ámbito didr_write a la Authorisation API v3.
9. Este token se utiliza para realizar los mismos pasos que antes, pero para los métodos addVerificationMethod (para añadir claves adicionales como ES256) y addVerificationRelationship (para añadir relaciones authentication y assertionMethod).
10. La transacción se firma (la Wallet) y se devuelve a la API para que la difunda por la red (actualice la blockchain) mediante el método sendSignedTransaction.

11. Finalmente, ya estaría creado el ID, que puede usarse para acceder a aplicaciones y servicios habilitados para EBSI.

El proceso de emisión de una credencial en EBSI

1. Un titular inicia la emisión en el sitio web del emisor, selecciona la credencial que quiere.
2. Las carteras digitales (wallet) implementan el "endpoint" openid-credential-offer, este inicia el flujo si el emisor es considerado de confianza. La Oferta de Credenciales puede proporcionarse como un valor, donde la siguiente estructura de datos se agrega bajo el campo credential_offer. También puede proporcionarse como una referencia URI a través del campo credential_offer_uri, que resolverá a la misma estructura de datos con un tipo de contenido de application/json. Esto ocurre si se solicita la VC a la Wallet.
3. En caso de solicitar la VC a un sitio Web se genera un QR
4. El usuario escanea el QR desde la Wallet
5. El cliente resuelve authorization_server y credentials_supported a través de la configuración de ./well-known/openid-credential-issuer. La configuración del emisor de credenciales tiene authorization_server apuntando hacia el Servidor de Autorización externo, con un client_id propio.
6. El cliente resuelve la configuración del servidor de autorización a través de la configuración ./well-known/openid del servidor de autorización. La configuración expone la configuración del servidor de autorización y cómo puede utilizarse.
7. El cliente procede con el flujo de emisión de credenciales verificables solicitando acceso para la credencial requerida al servidor de autorización. El objeto de solicitud debe firmarse con la clave privada del cliente, propiedad del client_id solicitante. La clave pública correspondiente debe poder resolverse a través de client_metadata.jwks_uri proporcionada en la solicitud de autorización inicial.

8. El Mock Auth valida la solicitud y procede solicitando la autenticación de un DID al cliente. La solicitud de token de identificación también es una solicitud de autorización y DEBE ser un objeto de solicitud firmado. El objeto de solicitud se firma con las claves privadas del servidor de autorización (simulador de autenticación), que se pueden encontrar a través del parámetro jwks_uri en ./well-known/openid-credential-issuer. La solicitud utiliza response_mode=direct_post y la ubicación de la respuesta se entrega en redirect_uri. La ubicación de redirección será la definida por el cliente client_metadata.authorization_endpoint o la predeterminada openid.
9. El cliente procede emitiendo un token de identificación firmado por la clave de autenticación del documento DID. Esto se utilizará para demostrar la identidad del sujeto mediante el control del DID. Si el cliente solicita VerifiableAuthorisationToOnboard, la firma no podrá validarse, ya que el documento DID aún no está registrado.
10. El Servidor de Autorización evalúa la respuesta de autenticación y la solicitud de autorización original para determinar si se debe conceder el acceso. Tras una autenticación correcta, el endpoint direct_post devuelve una redirección a la redirect_uri originalmente solicitada (paso 7) con un código.
11. El cliente procede con el flujo de código. El cliente llama a Token Endpoint con los detalles requeridos y firma client_assertion JWT con sus claves privadas. Las contrapartes de la clave pública deben poder resolverse a través de client_metadata.jwks_uri proporcionada en la solicitud de autorización inicial.
12. El token de acceso se entrega como una carga útil de respuesta de una iniciación correcta del punto final de token. c_nonce (Challenge Nonce) debe ser almacenado por el cliente hasta que se proporcione uno nuevo. El primer c_nonce puede transmitirse del servidor de autorización al emisor de conformidad a través de la credencial de acceso.
13. En este punto, el cliente ha obtenido con éxito un access_token válido, que puede utilizarse para acceder al punto final de credenciales del emisor de credenciales. El cliente solicita la emisión de la credencial

verificable al simulador de emisor. La Credencial solicitada debe ser igual al acceso concedido. La clave de autenticación del documento DID debe utilizarse para firmar la prueba JWT, y el DID debe ser igual al utilizado en la autenticación.

14. Después de la solicitud exitosa, la carga útil de respuesta contendrá la credencial solicitada.

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=ETS Ingenieros Informaticos - UPM, C=ES
	Fecha/Hora	Mon Jun 03 21:55:01 CEST 2024
	Emisor del Certificado	EMAILADDRESS=camanager@etsiinf.upm.es, CN=CA ETS Ingenieros Informaticos, O=ETS Ingenieros Informaticos - UPM, C=ES
	Numero de Serie	561
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)